

## INTERLOCAL AGREEMENT

THE STATE OF TEXAS     §  
                                     §  
COUNTY OF HARRIS     §

THIS INTERLOCAL AGREEMENT, made and entered into by and between HARRIS COUNTY, "County," a body corporate and politic under the laws of the State of Texas, "County," and the Montgomery Police Department, "Participating Agency."

The County agrees to provide the Participating Agency with access to and use of the information maintained by Southeast Texas Crime Information Center, "SETCIC," as a Stand Alone, Full Service Participant as the term is defined in the Policies and Procedures of SETCIC, a copy which is attached as Exhibit "A" and made a part of this Agreement by reference. To the extent the Participating Agency desires to switch the method of connecting to the SETCIC from a Stand Alone terminal to another method that is or may become available during the term of this Agreement, the Participating Agency shall make a written request to the Harris County Justice Technology Committee for approval. Additional connection methods include, but are not limited to, TLETS and JWEB.

### II.

With regards to its usage of the SETCIC system, the Participating Agency agrees to do the following:

- A. Abide by the rules, regulations, policies and procedures governing SETCIC, promulgated by the Harris County Justice Technology Committee, attached as Exhibit "A," and applicable to a Stand-Alone Full Service Participant that is not a County-funded agency;
- B. Work in concert with other participants in SETCIC in serving outstanding criminal warrants;
- C. Work in concert with the Harris County Justice Technology Committee in maintaining and improving SETCIC;
- D. Provide the necessary hardware and software to cause its computer to communicate with SETCIC via the protocol required by the County; and
- E. Provide the secure internet access to communicate with the County's computer network.

### III.

Upon execution of this Agreement, the County agrees to furnish the Participating Agency a list of transaction codes and/or system message key mnemonics to enable authorized employees and agents of the Participating Agency's law enforcement branch to obtain access, for full service, to the information in SETCIC. The Participating Agency agrees to provide the County with a list of names and business addresses of all authorized terminal

operators, computer operators, programmers, administrative staff and other data processing employees who will have access to SETCIC for full service.

- A. If the communications protocol used by the Participating Agency causes the Participating Agency's computer to connect to SETCIC through JWEB, in addition to the above-described, unique passwords shall be assigned to the appropriate personnel, by JWEB Security.
- B. If the communications protocol used by the Participating Agency causes the Participating Agency's computer to connect to SETCIC through the TLETS network, no passwords are issued in addition to the above-described certification by JWEB.

Use of a password for access to SETCIC by any person other than the owner of the password or use of SETCIC by a person or persons not authorized by JWEB is grounds for termination of this Agreement pursuant to Paragraph IV.

#### IV.

The term of this Agreement is perpetual, beginning on the date of execution, which is written just above the signatures below, and shall remain in force unless it is terminated by either party giving the other party thirty (30) days prior written notice of its intent to terminate. Notwithstanding the foregoing, the County reserves the right to terminate this Agreement immediately upon the occurrence of one or more of the following:

- A. Use of the Participating Agency's equipment to obtain information from SETCIC by any person who has not been assigned a password or otherwise authorized to have access to the SETCIC system by the Harris County Justice Technology Committee.
- B. Use of the Participating Agency's equipment to obtain information from SETCIC by any person who accesses SETCIC by utilizing another person's password;
- C. Any attempt to gain access through the Participating Agency's computer and associated equipment to information in SETCIC that is not authorized by; the Harris County Justice Technology Committee;
- D. If the computer capacity of SETCIC is inadequate to meet the computer needs of both the County and the Participating Agency and that condition continues for a period of thirty (30) days; or
- E. Violation of any rules, regulations, policies and/or procedures for SETCIC as established and as may be amended by the Harris County Justice Technology Committee.

#### V.

With regard to use of SETCIC, it is expressly understood and agreed that the Participating Agency has access only to the information available to it through the transaction codes and/or system message key mnemonics provided to it by the County, for law enforcement purposes only, and to no other computer data without written consent of the County. Further, it is understood that the dissemination or release of confidential information to any law enforcement agency, peace officer, or individual is governed by local, state and/or federal rules, regulations, statutes, and judicial decisions.

#### VI.

The Participating Agency has access to SETCIC twenty-four (24) hours a day, each and every day of the week, except during the time periods reserved for maintenance. The County is not liable for any temporary inability of the Participating Agency to obtain access to SETCIC due to maintenance, breakdowns, and other causes beyond the control of the County. In the event that the capacity of SETCIC is inadequate to meet the needs of the Participating Agency and the County, the rights of the County prevail.

#### VII.

The County neither guarantees nor is it responsible for the accuracy or timeliness of the information contained in SETCIC and in the event of mistake or inaccuracy, the County bears no liability. Further, the Participating Agency agrees to verify the accuracy of records with the office of the appropriate law enforcement agency that has in its possession the original warrants of arrest. **FAILURE TO VERIFY THE ACCURACY OF RECORDS WITH EACH LAW ENFORCEMENT AGENCY PRIOR TO THE EXECUTION OF A WARRANT OF ARREST IS GROUNDS FOR TERMINATION OF THIS AGREEMENT.**

#### VIII.

The Participating Agency agrees that it is responsible for the acts or failure to act of its employees, agents, or servants in regard to any use (authorized or unauthorized) of the Participating Agency's terminal and/or printer by the Participating Agency or any person; provided however, such responsibility is subject to the terms, provisions and limitations of the Constitution and laws of the State of Texas, chiefly the Texas Tort Claims Act.

#### IX.

The Participating Agency agrees to keep its terminal(s) and printer(s) functioning at an acceptable level so as not to interfere with SETCIC. Failure to do so is grounds for termination.

#### X.

The County reserves the right to delete or modify information contained in SETCIC that is made available to the Participating Agency. Furthermore, the County reserves the right to change the transaction codes and programs from time to time. If a change directly affects the Participating Agency, the County agrees to give written notification of that change to the Participating Agency not less than ten (10) days prior to the change.

XI.

All notices and communication shall be mailed by certified mail, return-receipt requested, or hand delivered to the parties at the following addresses:

FOR THE COUNTY:           Commissioner's Court of Harris County  
                                  Harris County Administration Building  
                                  1001 Preston, 9<sup>th</sup> Floor  
                                  Houston, Texas 77002

With a copy to:           Harris County Universal Services  
                                  406 Caroline, 2<sup>nd</sup> Floor  
                                  Houston, Texas 77002

FOR THE                   Montgomery Police Department  
PARTICIPATING           101 Old Plantersville Rd  
AGENCY:                  Montgomery, Texas 77356

These addresses may be changed upon giving prior written notice. Notices are deemed given upon deposit in the United States mail.

XII.

The Participating Agency agrees to comply with federal law and regulations, state law and administrative code, rules, procedures, and policies, now in effect or in the future formally approved and adopted by CJIS or Texas Department of Public Safety (TXDPS) in regard to any criminal justice information furnished through systems accessing CJI, as further described in the MOU attached hereto as Exhibit B.

XIII.

This Agreement is governed by the laws of the State of Texas. The exclusive forum for any action arising out of, in connection with, or in any way relating to the Agreement is in a state or federal court of competent jurisdiction in Texas. The exclusive venue for any action arising out of, in connection with, or in any way relating to the Agreement is in a state or federal court of competent jurisdiction in Houston, Harris County, Texas.

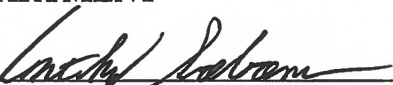
XIV.

This instrument contains the entire Agreement between the parties relating to the rights granted and the obligations assumed. This Agreement is not effective until it is signed by both Parties. Any oral representations or modifications concerning this Agreement are of no force or effect excepting a subsequent modification in writing signed by all parties.

IN TESTIMONY OF WHICH, this Agreement has been executed in duplicate originals, each to have the same force and effect, as follows:

A. It has been executed on behalf of Harris County on the \_\_\_\_\_ day of \_\_\_\_\_, 2022, by the County Judge of Harris County, Texas, pursuant to an order of the Commissioners Court of Harris County, Texas, authorizing such execution; and

B. It has been executed on behalf of the Montgomery Police Department on the \_\_\_\_\_ day of \_\_\_\_\_, 2022.

<b>MONTGOMERY POLICE DEPARTMENT</b>  BY:  NAME: <u>ANTHONY SOLOMON</u> TITLE: <u>CHIEF OF POLICE</u> DATE: <u>MAY 12, 2022</u>	<b>HARRIS COUNTY</b>  By: _____ LINA HIDALGO COUNTY JUDGE
	APPROVED AS TO FORM: CHRISTIAN D. MENEFE COUNTY ATTORNEY  By: _____ Cherelle Sims Assistant County Attorney C.A. File 22GEN1714

**EXHIBIT A**

**SETCIC Rules, Regulations, Policies and Procedures**

**(follows behind)**

**Harris County  
Justice Technology Committee**

---

**Southeast Texas Crime Information Center  
(SETCIC)**



**Applicant Information Packet**

## Table of Contents

Overview .....	1
Requirements for Participation .....	2
Access Methods .....	2
User Fees for Entering Agencies .....	2
Policies and Procedures .....	2
I.    General .....	3
II.   Operational .....	4
III.  Security .....	5
Policy Making, Enforcement .....	7
Application for Participation, Contracts .....	7
Sanctions, Cessation of Services .....	8
Participating Agency Access .....	8
Data Integrity, Data Control .....	8
User Fees - Annual, Monthly .....	8
Format and Data Content .....	9
Access by Harris County Funded Agencies .....	9
Effect Upon Existing Warrant System .....	9
SETCIC Identification Number (SID) .....	10
Cross-Reference and Indirect Access .....	10
Inquiries to SETCIC System .....	11
Record Retrieval For Update .....	11
Confirmation of Warrant Validity .....	12
Security - Access to SETCIC .....	12
Participating Agency System Identifier .....	12
Access to JWEB .....	12
System Availability .....	13
System Availability - Scheduled Downtime .....	13
SETCIC Agencies .....	13
System Demonstrations .....	14
Application Information .....	14

# **Southeast Texas Crime Information Center (SETCIC)**

## **Overview**

### **Introduction**

The Southeast Texas Crime Information Center (SETCIC) is the product of a long-term cooperative effort between the Harris County Commissioner's Court, the Harris County Justice Technology Committee, and the Area Chiefs of Police. The system is an automated central repository for law-enforcement data that allows single-point query for criminal justice information.

The SETCIC open warrant system went online September 1, 1984. It allows agencies in the Southeast Texas region to share information and apprehend people with outstanding criminal warrants. Through SETCIC, agencies can clear open warrants and generate revenue by collecting outstanding fines.

Agencies become SETCIC members by filling out an application, receiving approval from the Justice Technology Committee and the Harris County Commissioners' Court, and signing a contract. There are two types of participation in SETCIC – full service and inquiry only. Full-service agencies enter information and make inquiries. Fees are required for the data entry. Inquiry-only agencies access records, but do not make any entries. There are no fees for inquiring.

For each full-service agency, reports are generated monthly listing warrants entered, warrants located, and warrants cleared, among other things. Inventories of all an agency's Active SETCIC warrants can be produced upon request. However, the online SETCIC system does not maintain any history of warrants cleared, recalled, or deleted.

The system is intended to be self-supporting through the collection of annual user fees from full service agencies. It is also intended to be cost effective by using equipment that agencies currently have connected to the Department of Public Safety's communication switcher in Austin.

## **Requirements for Participation**

To become a SETCIC participant, and agency must:

1. Complete and return a SETCIC application (attached).
2. Execute a contract with Harris County regarding SETCIC.
3. Pay an annual fee for warrant entry.
4. No fee for inquiry only.

## **Access Methods**

There are two (2) methods of connecting to the SETCIC system.

1. Stand-Alone Terminal - existing hardware connected to the Texas Law Enforcement Telecommunications System (TLETS) maintained by DPS in Austin.
2. Internet Explorer web browser – personal computer connected to SETCIC through JWEB.

## **User Fees for Entering Agencies**

Fees are collected from agencies that enter warrants into SETCIC. These fees serve two purposes:

1. Offset a portion of the annual county expenditure for technical personnel to support and enhance the system.
2. Provide for self-funding for future computer hardware and replacement and enhancement to provide adequate user service.

The fees are as follows:

1. Annual participation fee of \$3000.00 for full service agencies.
2. Service fee of \$.20 per warrant entered during the monthly period.
3. Monthly service fee of \$3.00 per warrant located.
4. No annual fee for inquiry-only.

## **Policies and Procedures**

The Justice Technology Committee is the policy-making body for SETCIC.

# SETCIC POLICIES

## I. General

- A. All policies, procedures, and standards will be derived, issued and enforced by the Harris County Justice Technology Committee.
- B. Agencies wishing access to SETCIC will apply to the Justice Technology Committee for approval. Subsequently, the agency's SETCIC contract will be sent to the Harris County Commissioner's Court.
- C. Failure of any participant to comply with established policies and procedures will result in immediate cessation of services and all of the agency's records will be purged from the database.
- D. All non-Harris County participants will access SETCIC via the TLETS switcher maintained by DPS in Austin.
- E. Data integrity and control will be the responsibility of the agency that initially entered the data.
- F. File/record certification/validation procedures will be established regarding periodic file purges, requiring authorized signatures of agency heads for certain data retention.
- G. Full-service participants will be assessed an annual user fee established by the Justice Technology Committee.
- H. Full-service participants will be billed on a monthly basis an amount determined by a fixed formula based upon warrants served.
- I. All entries/inquiries will be automatically logged for billing and auditing purposes.
- J. The Justice Technology Committee may modify these policies at any time without giving prior notice.
- K. All reasonable attempts will be made to provide SETCIC user access twenty-four (24) hours a day, seven (7) days a week.
- L. Scheduled application downtime will occur as needed for enhancement and updates.
- M. Non-Harris County funded agencies will hold persons arrested on other agency warrants for a period not to exceed eight (8) hours after verification of warrant validity and notifying originating agency that person is in hand.

- N. Non-Harris County funded agencies will allow Harris County agencies to place persons arrested on a third agency's warrant in their jail facility after verification of warrant validity and notification of originating agency that person is in hand.
- O. Non-Harris County funded agencies arresting a person on a Harris County warrant will upon verification of warrant validity and notification of appropriate county agency do one of the following:
  - 1. Deliver the person to the Harris County Joint Processing Center.
  - 2. Deliver the person to the nearest outlying Harris County Jail.
  - 3. Deliver the person to county personnel at a place and time agreed upon by both parties.
- P. Harris County agencies arresting a person on a non-county agency warrant will, upon verification of warrant validity and notification of originating agency, either:
  - 1. Deliver the person to originating agency personnel at a place and time agreed upon by both parties.
  - 2. Deliver the person to the jail facility of the nearest participating agency for originating agency pick up.

## **II. Operational**

- A. Update and inquiry formats and data content for stand-alone, TLETS-connected devices will be as nearly identical to existing TCIC/NCIC formats as possible to facilitate entry/inquiry to SETCIC, TCIC, NCIC in single operations from the user terminal.
- B. Data elements, edit and verification criteria will be identical to those used in TCIC/NCIC except where SETCIC requirements dictate data or edits beyond those required by TCIC/NCIC. In such cases, SETCIC edit and verification criteria will prevail.
- C. Sheriff's and Constables' Office warrant system processing procedures should not change as a result of implementation of SETCIC. Update of SETCIC will be automatic with warrant acknowledgement /execution.
- D. Each warrant entered will be assigned a unique SETCIC identifier (SID) for future record manipulations.
- E. Records will be stored in a keyed sequence of the assigned SETCIC identification number unique per record. This is required data on all records create/update operations.
- F. Cross-references will be maintained using driver license number, social security number, alien registration number, JWEB SPN when available, or other identifiers.

- G. Inquiries into the system can be made by name with or without identifiers, by SETCIC ID number, or by existing cross-reference numbers.
- H. Inquiry can be made using partial key data for a return of possible matches. This list would then be used to determine the actual key to be used.
- I. Record retrieval for update purposes will require SETCIC ID number or exact match of name, race, sex, date-of-birth and:
  - 1. Entry Agency Identifier
  - 2. Originating Agency Case Number
- J. Initial warrant entry into system will require as minimum data:
  - 1. Originating Agency Identifier (ORI)
  - 2. Defendant's Name
  - 3. Race
  - 4. Sex
  - 5. Date of Birth
  - 6. Offense
  - 7. Date of Warrant
  - 8. At least one of the following:
    - a. Driver's License Number
    - b. Social Security Number
    - c. Official DPS ID Number
    - d. Alien Registration Number
- K. Upon receiving a positive response to a SETCIC inquiry, the requesting agency must immediately confirm with the originating agency that the warrant is valid and in force.

### **III. Security**

- A. Access to SETCIC files and functions will be limited to authorized agencies.
- B. The agency identifier will be the TCIC originating agency identifier (ORI).
- C. Harris County Universal Services (HCUS) will operationally maintain any security files, programs and reports under the control of the Justice Technology Committee.
- D. Agencies will be allowed inquiry or update capability, or both based upon approval of the Justice Technology Committee and upon execution of an approved contract with Harris County. Security profiles will be established and maintained to disallow unauthorized activity.

- E. Sanctions regarding security violations or attempted unauthorized activity will be established and enforced by the Justice Technology Committee and may include removal of the participating agency from SETCIC.
- F. All entries/inquiries will be automatically logged for security auditing purposes. Information captured will include but not be limited to:
  - 1. Agency identifier
  - 2. Operation
  - 3. Selection information supplied
  - 4. Hit/no-hit information
  - 5. Security breach attempt indicator
  - 6. Date/time
- G. No access to the files and/or records of the Harris County JWEB Criminal or Civil applications will be allowed via the state network unless specifically approved by the Justice Technology Committee.
- H. Necessary system software and file implementation, maintenance, and monitoring will be performed by the personnel of HCUS under specific contract or agreement with the Justice Technology Committee and Commissioners' Court.
- I. Hardware housed by the HCUS will be secured under terms of the aforementioned contract or agreement.

# **SETCIC PROCEDURES**

## **Policy Making, Enforcement**

(See I-A, I-J)

The Justice Technology Committee will approve modifications to the SETCIC policies on an as-needed basis. Recommendations will be included as regular agenda items for each monthly meeting, and effective upon approval. Recommendations may be formulated by any or all the following:

1. Justice Technology Committee prerogative.
2. Changes to the automated system requiring policy modification.
3. Actions taken by the user group forwarded for approval.
4. Commissioners Court action changing basic law enforcement procedures.
5. Legislative action.

Upon Justice Technology Committee adoption of policy changes the Justice Technology Committee will amend the policies as required and forward updates to all participants and other interested parties.

## **Application for Participation, Contracts**

(See I-B, III-D)

Completion of and submission to the Justice Technology Committee of the SETCIC Agency Application form (Attachment A) will constitute formal application for participation in the SETCIC program.

All applicable information must be included. The application should be signed by the Chief Law Enforcement Officer or agency executive officer.

The Justice Technology Committee will review the SETCIC application. After approval, the HCUS will request that the County Attorney's Office prepare a contract to be presented to the Harris County Commissioners' Court for approval and execution. The executed contract will be forwarded to the governing body of the participating agency for approval and execution.

A full-access agency will be allowed access to SETCIC once HCUS receives the executed contract and the annual user fee.

An inquiry-only agency will be allowed access to SETCIC once HCUS receives the signed user agreement.

## **Sanctions, Cessation of Services**

(See I-C, II-E, III-E)

Each participating agency will be required to follow all rules, regulations, policies, and procedures adopted by the Justice Technology Committee. Failure to comply may result in cessation of SETCIC services due to Justice Technology Committee action.

Violations may be determined via system management reporting, notification of violation from the user group or other methods. The Justice Technology Committee will consider each violation and/or report on its merit and direct the HCUS to take action based on its majority decision.

Should the action of the Justice Technology Committee be to terminate service to the participating agency, HCUS will immediately notify the agency by phone and follow up with written notice.

## **Participating Agency Access**

(See I-D)

Two methods of SETCIC access are available:

1. Stand-alone device connected to TLETS switcher maintained by DPS in Austin.
2. Internet access through Internet Explorer web browser

Use of existing TLETS-connected equipment is an economical method of connecting to SETCIC since most equipment is owned and DPS pays line costs.

Interface with the SETCIC application must be made in accordance with specifications supplied by the HCUS.

## **Data Integrity, Data Control**

(See I-E, I-F, II-E, II-F, II-M)

The quality of data resident on SETCIC files will dictate the quality of the system. It is imperative that errors be corrected immediately.

Data entered into the system is the responsibility of the entering agency. Reports will be routinely generated pointing out potential errors that must be corrected immediately. Records that are not corrected will be purged from the system.

## **User Fees - Annual, Monthly**

(See I-C, I-G, I-H)

Full-access agencies will be charged a three-thousand dollar (\$3000.00) annual SETCIC access fee. This fee must be remitted not more than ten (10) days after execution or renewal of the SETCIC contract.

Failure to remit will result in the cessation of services and the purge of all records in SETCIC.

Full-access agencies will be assessed a monthly fee by invoice amounting to the prevailing per warrant fee multiplied by the number of warrants served or located by an agency other than the originating agency plus twenty cents (\$.20) per warrant entered.

Failure to remit payment to Harris County within 10 days of invoicing will result in the cessation of services and the purge of records in SETCIC.

All remittances should be made to Harris County in care of the Public Safety Technology.

Resumption of services will be subject to Justice Technology Committee approval and may require remittance of the annual fee for reinstatement.

### **Format and Data Content**

(See II-A, II-M, II-B, II-E, II-F, II-G, II-H)

SETCIC was designed for ease of use by persons accustomed to the TCIC and NCIC systems and the format of response screen will be very similar to TCIC/NCIC. Input data and edit criteria will closely resemble TCIC/NCIC. The purpose is to reduce the training process and provide immediate operator productivity.

Required data for warrant input matches TCIC/NCIC but additional data can be input to improve system service. Detailed information is available in the SETCIC Entry manual.

In situations where SETCIC and TCIC/NCIC requirements may differ, SETCIC will prevail in regard to data and procedures.

### **Access by Harris County Funded Agencies**

(See II-C, III-A, III-C)

Criminal Justice agencies will access SETCIC via Internet Explorer web browser. The number and placement of workstations will be determined by each agency. Security clearances will be provided by the departmental Security Administrator as is currently done for the JWEB system.

Access to SETCIC by any Non-Criminal Justice agency is disallowed unless expressly considered and approved by the Justice Technology Committee

### **Effect Upon Existing Warrant System**

(See II-D)

SETCIC will not affect the JWEB warrant subsystem processing. All Harris County warrants are added to and removed from SETCIC files via automatic program functions.

Warrants held by Harris County law-enforcement agencies but not entered into JWEB can be directly entered into SETCIC and must be removed from SETCIC upon execution or cancellation.

## **SETCIC Identification Number (SID)**

(See II-G, II-H, II-J, II-L)

Each warrant entered into SETCIC will be given a unique, computer-generated number. This number is the direct-access identifier for the warrant. All updates, locates, clears, and cancellations will be performed using this number.

After a warrant is entered, the SID will display at the bottom of the screen. The SID should be written on the physical document, envelope or folder and used for future reference.

## **Cross-Reference and Indirect Access**

(See II-I, II-J, II-M)

Several identifying numbers can be entered into SETCIC for cross-reference and indirect access. These numbers include:

1. Social Security Number
2. Driver's License
3. Alien Registration Number
4. Originating Agency Case Number
5. JIMS System Person Number (SPN)

Operators may inquire using cross-reference numbers. Matches will be returned if available.

Multiple identifying numbers may be attached to a single warrant. All the identifiers above can be used together in any combination. When an operator inquires on an identifying number that has been entered into SETCIC, the warrant record will display.

## **Inquiries to SETCIC System**

(See II-I, II-J, II-K, II-M)

Since SETCIC was designed along the lines of TCIC/NCIC, inquiries can be made with a name and personal descriptors as follows:

1. Full name with race, sex, date of birth.
2. Partial name (example: last name, first initial) with race, sex, date of birth.
3. Name and any combination of descriptor information.
4. Name or partial name only.
5. SETCIC identification number (SID).

Any inquiry formats other than 1 or 5 will result in lists of "possible" matches requiring further system query.

Identifying numbers that have been entered into a SETCIC warrant record may be used to retrieve a record.

## **Record Retrieval For Update**

(See II-L, III-D, III-E)

To modify or update a SETCIC warrant record, use one of the following:

1. SETCIC Identification Number (SID).
2. Full, exact name, race, sex, date of birth, originating agency identifier (ORI) and agency case number.

These are the only two access methods that ensure that the exact record is updated. Use of the SID is preferred and recommended for system and operator efficiency.

Updates are defined as:

1. Modification
2. Locate
3. Clear
4. Cancel
5. Reset     This operation will activate a warrant that was previously cancelled.

## **Confirmation of Warrant Validity**

(See I-A, I-C, II-N)

On the Warrant Detail screen, a current telephone number for the originating agency will display. Call this number to confirm the validity and current state of the warrant. Always confirm a warrant before taking any action on the warrant.

When an agency arrests or detains a person and determines that the person has outstanding warrants in other jurisdictions, the arresting agency must immediately contact the originating agency for confirmation. This confirmation may be completed by telephone or through the administrative messages function.

The originating agency must respond within ten (10) minutes to any request for confirmation. Should an agency not respond, the arrested person may be released, and notation of the event logged by the arresting agency.

Verbal confirmation of warrants, either by phone or radio, must be followed by written notice of confirmation, either by fax or teletype, within 30 minutes, if requested by the arresting agency.

Note: No person will be incarcerated in any Harris County jail facility unless the original warrant accompanies the arrested person.

## **Security - Access to SETCIC Participating Agency System Identifier**

(See I-B, III-A, III-B, III-C, III-D, III-E)

No agency may use the SETCIC system unless that agency has applied for access, obtained Justice Technology Committee approval, signed a contract with Harris County, and been notified by the HCUS that the agency is cleared for operation.

The HCUS SETCIC section will maintain control of all system security files and programs.

Security will be maintained using the originating agency identifier (ORI) as control data in conjunction with approved terminal identifiers.

The ORI will also determine the offense classification the agency is allowed to enter. County agencies are allowed to enter all classes of offenses from misdemeanor class C through felonies.

Municipalities will typically be allowed to enter class C misdemeanors. The level of offense classification is set at the time system access security clearance is provided.

## **Access to JWEB**

(See III-G, I-D)

SETCIC participants may not access the other JWEB Systems.

To obtain access to JWEB Criminal and Civil System files, an agency must apply to and obtain approval from the Justice Technology Committee, request a unique system sign-on code for each

operator, and obtain security clearance.

## **System Availability**

(See I-K, I-L, I-M)

SETCIC is designed to improve law-enforcement and officer safety. All practical attempts will be made to provide access twenty-four (24) hours per day, seven (7) days per week.

Exceptions must be made for regular system and file maintenance. Normal downtimes will occur weekly at a time determined by users as that having the least impact.

Exceptions will also appear in the form of hardware malfunctions, communication line problems, and software failure. These must be handled on an individual basis and necessary steps taken to remedy the problem.

## **System Availability - Scheduled Downtime**

(See I-L)

System, file and hardware maintenance will require a downtime period on a weekly basis. The downtime periods should not be longer than one (1) hour at the onset but may become longer as file sizes increase.

The reason for the downtime is to clean the files of records that are in a removable or purgeable condition. If this is not done regularly, file space for new records would rapidly decrease and the time required to rebuild files and search for records would increase.

Currently, downtimes are scheduled for Wednesdays at 5:00 - 6:00 AM as needed. This time frame was chosen based upon expected low activity at this day/time.

Any changes to the downtime schedule will be the result of majority consensus of the collective users.

Problems may occur from time to time which are not foreseeable, or which are known in advance to require extended downtime of the system.

## **SETCIC Agencies**

A list of the agencies can be requested by contacting one of the persons listed below:

### **I. Full-Service Agencies**

Refers to duly contracted agencies that have paid all required annual and monthly fees and been allowed access to all SETCIC systems and files, with update and inquiry capabilities.

### **II. Inquiry-Only Agencies**

Refers to all agencies allowed access to selected SETCIC systems and files with query

capability only (no update functions). These agencies have executed a user agreement and been approved by the Justice Technology Committee.

## **System Demonstrations**

Agencies interested in "hands-on" demonstrations of the SETCIC system are invited to contact.

1. (US) JWEB SETCIC

E-mail: [usjwebsetcic@hctx.net](mailto:usjwebsetcic@hctx.net)

## **Application Information**

Email: JWEB\_SETCIC\_Access@us.hctx.net



Harris County Justice Technology Committee  
Southeast Texas Crime Information Center  
Agency Application

Date: 01-27-2022

Agency: Montgomery Police Department

State ID: TX ORI: TX 1701700 Jurisdiction Population: approx 2100

Agency or Department Head: Anthony Solomon, Chief of Police

Agency Contact:

Name: Albert Chambers Title: Police Sergeant Detective

Phone: (936) 597-7259 E-mail: achambers@ci.montgomery.tx.us

Address: 101 Old Plantersville Rd

City: Montgomery County: Montgomery State: Tx Zip: 77356

Number of Police Officers:

Total: 15 Field: 14 Reserve: 1

Check the Level of Access Desired: ☒ Full Service (Entry and Inquiry) ☐ Inquiry Only

Warrant Verification Hours:

☒ 24 hours ☐ From \_\_\_\_\_ a.m. / p.m. To \_\_\_\_\_ a.m. / p.m.

Warrant Verification Phone Number: (936) 449-0536 (nighttime only) 936-597-6434

Terminal Information:

Number of Terminals Connected Directly to SETCIC: N/A

Number of Terminals Connected to SETCIC Via TLETS: 1

Terminal IDs or TLETS Addresses

MGPZ 10.42.2.195

Authorization:

Requested By: A. Chambers Signature: A. Chambers

Agency Chief Executive: Anthony Solomon

Agency Attorney: Cable D. Villanar

SETCIC Use Only

Date Received: \_\_\_\_\_

CC Approval Date: \_\_\_\_\_

Entered By: \_\_\_\_\_ Date Entered Into SETCIC: \_\_\_\_\_

**EXHIBIT B**

**CJIS Information Exchange MOU**

(follows behind)

## Regional Law Enforcement Agency CJIS Information Exchange Memorandum of Understanding

Harris County Sheriff's Office ("HCSO") and Harris County Universal Services ("HCUS") wish to establish guidelines through this Memorandum of Understanding for access to systems which provide CJIS information. HCSO desires to share access between law enforcement agencies within Harris County and law enforcement agencies in surrounding counties, in order to expand regional collaboration and strengthen information sharing capabilities.

### **I. AGREEMENT TO FOLLOW GUIDELINES**

The following MOU is made and entered into by and between the Parties, namely the

Montgomery Police Department, as identified by the federally assigned originating agency identifier (ORI) TX1701700, hereinafter referred to as "the Regional Agency";

Harris County Sheriff's Office; and Harris County Universal Services, the

Noncriminal Justice Agency (NCJA) providing technology services in support of HCSO, in accordance with a management control agreement.

This MOU sets forth the rights and responsibilities of the Parties with regard to the storage, exchange, and use of any information accessible via any connections to TLETS provided by HCSO and HCUS.

Any law enforcement agency desiring access to TLETS through applications made available by HCSO and HCUS hereby agrees to abide by these guidelines. This document shall be signed by an authorized representative of the law enforcement agency. All services shall only be used for appropriate law enforcement purposes and as allowed in these guidelines. Network access is provided for access to TLETS only.

### **II. TERM**

This MOU is a formal expression of the purpose and intent of both Parties and is effective when signed, and will remain in effect after the signatories vacate their positions or until it is affirmatively amended or rescinded in writing. This MOU does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

### **III. DEFINITIONS**

1. "CJT" shall mean criminal justice information, including, but not limited to, criminal history record information; motor vehicle and driver registration information; wanted, missing, and other person information; wanted and stolen property information; and other information used by criminal justice agencies to perform their missions.
2. "CJIS" shall mean the Federal Bureau of Investigation's Criminal Justice Information Services Division, being the repository for criminal justice information services in the Federal Bureau of Investigation. NCIC and III are systems managed by CJIS.
3. "NCJA" shall mean Noncriminal justice agency, an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.
4. "Regional Agency" shall mean the law enforcement agency gaining access to TLETS through applications or connections provided by HCSO and HCUS.
5. "TLETS" shall mean Texas Law Enforcement Telecommunications System, a statewide telecommunications network that is composed of city, county, state, federal, and military law enforcement and criminal justice agencies in Texas. The system is designed exclusively for use by criminal justice agencies in conducting their lawfully authorized duties within their respective jurisdictions and between agencies as required.

### **IV. DOCUMENTS INCORPORATED BY REFERENCE**

**The following documents are hereby incorporated by reference and made a part of this MOU:**

1. United States Code of Federal Regulations Title 28 Part 20 (28 CFR 20), as now enacted or hereafter amended;
2. CJIS Security Policy, as now published or hereafter amended;
3. Texas Security Policy Supplement  
(<http://www.dps.texas.gov/SecurityReview/TexasCJISSecurityPolicy.pdf>), as now published or hereafter amended.

The Parties hereby agree that these documents so incorporated may be amended at any time after this MOU takes effect, and that such amended documents shall have as much effect immediately as the originals of the same have at the time this MOU takes effect.

### **V. RESPONSIBILITIES OF REGIONAL AGENCY**

The Regional Agency shall do the following:

1. Appoint an employee of the Regional Agency to be a liaison to HCSO and HCUS to interact on any questions or issues arising under these guidelines. The name and contact information for the liaison shall be provided to HCSO when access is provided. Liaison information shall be updated as needed;
2. Comply with federal law and regulations, state law and administrative code, rules, procedures, and policies, now in effect or in the future formally approved and adopted by CJIS or Texas Department of Public Safety (TXDPS) in regard to any criminal justice information furnished through CJIS systems;
3. Meet or exceed all applicable security requirements as described in the CJIS Security Policy, now in effect or in the future promulgated; this includes, but is not limited to:
  - a) Access and use CJI for official criminal justice purposes only; and maintain a log or other auditable record of any secondary dissemination of CJI, in accordance with applicable CJIS policies;
  - b) Limit access to CJI to authorized Agency employees;
  - c) Prevent non-criminal justice personnel or personnel not under the management control of the Regional Agency from accessing CJI in any form, including printed, spoken, and electronic;
  - d) Ensure every individual within the scope of the Regional Agency's authority with direct or indirect access or exposure to CJI, in any form, including hardcopy, completes Security Awareness training before being provided access, and then every two years thereafter;
  - e) Prohibit and prevent any dissemination of CJI via unsecure electronic modes of communication, including, but not limited to, unencrypted mail, unencrypted file transfer, any unencrypted transmission over unsecure networks, or storage on unencrypted removable media, such as USB drives and CDs/DVDs;
  - f) Securely dispose of any media containing CJI, including, but not limited to, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items, by a process of shredding, incineration, degaussing, or secure erasure, as appropriate for the media to be destroyed;
  - g) Protect any Agency network or computer system transmitting or containing CJI from unauthorized access by use of an appropriate combination of firewalls, intrusion detection systems, and intrusion protection systems;
  - h) Maintain any and all such records as may be necessary to document compliance with the requirements of the CJIS Security Policy, and provide such documentation

upon request.

4. Regional Agency shall be responsible for any costs it incurs for access to TLETS systems.
5. Regional Agency agrees to work with HCUS to create and maintain network connectivity using approved solutions.
6. Regional Agency agrees to maintain CJIS compliance on its side of the connection, including its network access and terminals (security patches, anti-virus, etc.).
7. Regional Agency agrees to only access TLETS services from CJIS secure locations or using their own CJIS compliant remote access VPN solution.
8. Regional Agency is not authorized to provide TLETS access to any other entities not included in this agreement, or to any entities not within its IT administrative control, unless express written authorization is given by HCSO and HCUS.
9. Regional Agency must certify that network connections comply with standards of network configuration checklist provided in Attachment A.

#### **VI. GENERAL INFORMATION**

1. **Support:** Network support provided by HCUS is best effort.
2. **Negligence:** HCSO and HCUS are not responsible for malware or other exploits of Regional Agency originating from the Harris County network connection.
3. **REGIONAL AGENCY AGREES TO HOLD HARRIS COUNTY HARMLESS FROM ANY AND ALL LIABILITY, EXPENSE, JUDGMENT, SUIT, CAUSE OF ACTION, OR DEMAND, INCLUDED BUT NOT LIMITED TO ANY LIABILITY FOR DAMAGES BY REASON OF OR ARISING OUT OF ANY FALSE ARREST OR IMPRISONMENT OR ANY CAUSE OF ACTION, ARISING OUT OF OR INVOLVING ANY NEGLIGENCE ON THE PART OF THE REGIONAL AGENCY OR ANOTHER ENTITY OVER WHICH REGIONAL AGENCY EXERCISES CONTROL IN THE EXERCISE OF THIS AGREEMENT, TO THE EXTENT PERMITTED BY LAW.**

#### **VII. DISCONNECTION**

If Regional Agency no longer desires access to TLETS systems, it shall immediately notify HCSO or HCUS to coordinate disconnection. If it shall come to the attention of HCSO or HCUS that access to TLETS systems is being used in an inappropriate or unlawful manner HCSO and HCUS shall have the right to terminate the access connection immediately. Upon cancellation, Regional

Agency is no longer entitled to access TLETS through connections or applications provided by HCSO and HCUS.


In consideration for the use of TLETS systems described herein, an

authorized representative of MONTGOMERY POLICE DEPARTMENT  
(Name of Regional Law Enforcement Agency)


hereby binds said agency to follow the conditions stated herein.

[Signature Page Follows]

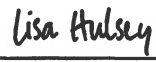
**REGIONAL LAW ENFORCEMENT  
AGENCY**

By:   
Signature Authorized Representative  
Name: Anthony Solomon  
Title: Chief of Police  
Date: May 12, 2022  
Agency: Montgomery Police Department


**HARRIS COUNTY SHERIFF'S OFFICE**

By:   
Ed Gonzalez  
Sheriff  
Date: 6/15/2022


APPROVED AS TO FORM:  
CHRISTIAN D. MENEFE  
COUNTY ATTORNEY

By:   
Lisa Hulsey  
Senior Assistant County Attorney

**HARRIS COUNTY  
UNIVERSAL SERVICES**

By:   
MG Richard J. Noriega (Ret)  
Executive Director  
Date: 07/08/2022

APPROVED AS TO FORM:  
CHRISTIAN D. MENEFE  
COUNTY ATTORNEY

By:   
Cherelle Sims  
Assistant County Attorney  
CA File No. 20GEN0142

**ATTACHMENT A**  
**“Network Configuration Checklist”**  
**(follows behind)**

## Network Configuration Checklist

Please complete the following questionnaire to indicate the status of CJIS Policy requirements as they pertain to your agency.

Email Address: **jbelmares@ci.montgomery.tx.us**

1. Does your agency have a process in place to ensure that all personnel who are granted access to CJI will receive security awareness training within six months of initial assignment and biennially thereafter?  
☒ YES   ☐ NO
2. If non-criminal justice personnel have access to your agency's facility, have you conducted background clearances, including fingerprinting on those personnel?  
☒ YES   ☐ NO
3. Does your agency have a documented incident handling and response plan?  
☒ YES   ☐ NO
4. Does your agency have a written and enforced policy for creating, activating, disabling and removing accounts with CJI access?  
☒ YES   ☐ NO
5. Does your agency have a written and enforced policy that prohibits sharing of user IDs and passwords?  
☒ YES   ☐ NO
6. Does your agency have a domain policy that locks out a user account after a number of consecutive invalid network access attempts?  
☒ YES   ☐ NO
7. Does your agency enforce a session lock on user workstations after a period of inactivity, and does the session lock remain in effect until the user reestablished access using appropriate identification and authentication procedures?  
☒ YES   ☐ NO
8. Does your agency's password rules on workstations and MDTs include specific requirements for minimum length, composition/complexity, password aging/expiration, and password protection that meet the CJIS password requirements?  
☒ YES   ☐ NO

9. Does your agency have a formalized patch management process to ensure that security updates are automatically applied to user workstations in a timely manner?  
☒ YES ☐ NO
10. Are all of your agency's IT systems protected with antivirus, antispyware and spyware protection, and configured to receive automatic updates of new virus definitions as they are made available?  
☒ YES ☐ NO
11. Does your agency's facility have physical and personnel security controls sufficient to protect CJI?  
☒ YES ☐ NO
12. Does your agency share a facility with any non-criminal justice agencies?  
☒ YES ☐ NO
- a. If so, what agencies?  
City Hall Administrators
- b. Is your agency physically segmented from these agencies?  
☒ YES ☐ NO
- c. How is physical access between the facilities controlled?  
Security Door with Keypad Lock
13. Does your agency have a boundary protection device (firewall) implemented to protect computers and access devices from non-CJI networks?  
☒ YES ☐ NO
14. Does your agency share a network with any non-criminal justice agencies?  
☐ YES ☒ NO
- a. If so, is your traffic segmented and/or encrypted?  
☐ YES ☐ NO
15. Does your agency have any wireless access points (APs) connected to your network?  
☒ YES ☐ NO
- a. If yes, has security been enabled and configured on the APs so that access is restricted through user authentication and encryption mechanisms?  
☒ YES ☐ NO
16. Does your agency have mobile devices (MDTs) or do any other agencies MDTs connect to your network?  
☒ YES ☐ NO
- a. If so, please describe how the MDTs connect to the network, and how they authenticate.  
MDT's are connected to a secure Verizon MiFi
- b. Are the MDTs secured in the vehicle by a locking vehicle mount?  
☒ YES ☐ NO

- c. If no, is your agency using advance authentication to further secure MDTs?  
☐ YES   ☐ NO
- d. Is data that is transmitted to/from MDTs protected with encryption?  
☒ YES   ☐ NO
- 17. Are personal/software based firewalls enabled and kept up-to-date on all wireless laptop devices and MDTs?  
☒ YES   ☐ NO
- 18. Does your agency have a Network Diagram which lists all communications paths, circuits, and other components that will be or are being used to access CJIS system?  
☒ YES   ☐ NO
- 19. Does your agency have formal, written procedures that require the secure disposal or destruction of physical and electronic media?  
☒ YES   ☐ NO

Please provide further explanation of your answers, as necessary in the notes section below:

The City of Montgomery Hall and Police Department has a contract with a secure shredding company.

ORDER OF COMMISSIONERS COURT  
Authorizing Interlocal Agreement

The Commissioners Court of Harris County, Texas, met in regular session at its regular term at the Harris County Administration Building in the City of Houston, Texas, on \_\_\_\_\_, with all members present except \_\_\_\_\_.

A quorum was present. Among other business, the following was transacted:

ORDER AUTHORIZING EXECUTION OF INTERLOCAL AGREEMENT  
WITH MONTGOMERY POLICE DEPARTMENT

Commissioner \_\_\_\_\_ introduced an order and moved that Commissioners Court adopt the order. Commissioner \_\_\_\_\_ seconded the motion for adoption of the order. The motion, carrying with it the adoption of the order, prevailed by the following vote:

	Yes	No	Abstain
Judge Lina Hidalgo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comm. Rodney Ellis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comm. Adrian Garcia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comm. Tom S. Ramsey, P.E.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comm. R. Jack Cagle	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The County Judge thereupon announced that the motion had duly and lawfully carried and that the order had been duly and lawfully adopted. The order adopted follows:

IT IS ORDERED that:

1. The Harris County Judge is authorized to execute on behalf of Harris County an Interlocal Agreement between Harris County and Montgomery Police Department to have Stand Alone Full Service access to the County's SETCIC application at no cost to the County. The Agreement is incorporated by reference and made a part of this order for all intents and purposes as thought set out in full word for word.
2. All Harris County officials and employees are authorized to do any and all things necessary or convenient to accomplish the purposes of this order.