TEXAS GANG INTELLIGENCE INDEX (TXGANG) USER AGREEMENT

This agreement is made and entered into between the Texas Department of Public Safety (DPS), which is responsible for the maintenance of the Texas Gang Intelligence Index (TxGang), and the Mission Police Dept. hereinafter referred to as the Participating Agency.

The DPS has established and maintains a statewide gang intelligence index, TXGANG, for the purpose of facilitating the investigation, prosecution, and/or punishment of criminal offenses relating to a criminal street gang. The Participating Agency entering into this User Agreement has read and fully understands the responsibilities of being a participating agency in TXGANG. The DPS reserves the right to suspend or terminate the use of TXGANG by any Participating Agency for any breach of the User Agreement.

The Participating Agency agrees to:

1. If applicable, comply with the Department of Justice Criminal Intelligence Systems Operating Policies 28 Code of Federal Regulations Part 23, Chapter 67 of the Texas Code of Criminal Procedure and the TXGANG Operating Policies and Procedures in regards to, but not limited to, submission, query, dissemination, and retention of records, training, and terminal and data security.

2. Establish a written policy applicable to the participating agency on TXGANG issues such as, record submission, removal, quality control, validation, dissemination, and system security.

3. Refrain from using information obtained from TXGANG to populate another intelligence or searchable database.

4. Ensure that all users that are provided access within the agency are authorized users, properly trained, and using appropriate electronic transmission.

5. Maintain a list of all authorized users and provide the list to the Administrator of TXGANG.

6. Maintain supporting documentation on submissions for as long as record remains in TXGANG.

7. Be responsible for the quality of the information submitted and for modifying or deleting a record if necessary.

8. Notify DPS immediately and execute a new User agreement upon a change in the chief executive officer or head of the Participating Agency.

Participating Agency acknowledges and agrees that all submissions of criminal intelligence information on individuals and organizations submitted to TXGANG are the property and responsibility of the submitting agency, not DPS. Participating agency acknowledges it has a duty to adhere to, if applicable, 28 CFR Part 23 and Chapter 67 of the Code of Criminal Procedure requirements including proper ID criteria for a gang member, proper criminal predicate for the gang, lawful acquisition of the information being submitted, effective control of dissemination only on a right and need to know basis and

maintaining proper records for each dissemination. TO THE EXTENT AUTHORIZED BY LAW, PARTICIPATING AGENCY SHALL INDEMNIFY AND DEFEND DPS FROM ALL DAMAGES ARISING OUT OF PARTICIPATING AGENCY'S PERFORMANCE UNDER THIS AGREEMENT CAUSED BY (1) ANY NEGLIGENT ACT OR OMISSION OR (2) WILLFUL MISCONDUCT OF PARTICIPATING AGENCY, ITS EMPLOYEES OR ANYONE FOR WHOSE ACTS PARTICIPATING AGENCY MAY BE LIABLE.

This agreement may be terminated by either the agency head or DPS at any time after providing 30 days written notice to the other party. Any changes to this agreement must be in writing and be mutually agreed upon by all parties.

This TxGang User Agreement will become effective on _____. (Date to be completed by DPS).

IN WITNESS WHEREOF, the parties hereto caused this TxGang User Agreement to be executed by the proper officers and officials:

PARTICIPATING AGENCY	PARTICIPATING AGENCY REPRESENTATIVES
Printed Name of Agency Head or Designee	Printed Name of Participating Agency Primary Representative
Signature	Signature
Title	
Date	Printed Name of Participating Agency Alternative Representative: Teodoro Rodriguez
ORI	Signature

1200 E 8th St. Mission, Texas 78572
Agency Address/City/Zip Code

TEXAS DEPARTMENT OF PUBLIC SAFETY

Michelle Farris
Printed Name

Chief
Title

Date

TXGANG SAMPLE GUIDELINES

Attached are sample TXGANG Guidelines that can be used as an outline by agencies in preparing their own TCIC/NCIC procedures manual. The TXGANG Manual and policies and procedures will provide your agency with a thorough explanation of each section in these guidelines. These guidelines are just a sample and must be adapted to fit the unique procedures of any agency choosing to use them. Agency guidelines must be placed on agency letterhead and the "sample" verbiage removed.

GENERAL

1. DPS operates TXGANG in accordance with the provision of CCP Ch. 67. CCP Ch. 67 requires that, if a law enforcement agency maintains criminal street gang information in a local or regional database, the agency must submit the information to TXGANG.
2. Each agency must ensure a current Texas Gang Intelligence Index (TXGANG) User Agreement is in place. TCIC auditors will require a copy of the agreement during an audit.
3. The agency administrator must ensure that individual user agreements for TXGANG access are current and accessible. Users must be disabled when access is no longer required.
4. Notify DPS immediately and execute a new User Agreement upon a change in the chief executive officer or head of agency.
5. All problems relating to TXGANG will be forwarded to the agency administrator for resolution.

TRAINING

1. Requires Title 28 Code of Federal Regulations training for ***ALL*** who input or retrieves info every 2 years. (A link to online CFR training is provided on the TXGANG website).
2. DPS will provide initial system training for TXGANG in addition to CFR training. DPS will facilitate training and provide technical updates, develop, update and provide access to TXGANG training materials.

SECURITY

1. Agency shall comply with the security provisions of the Criminal justice Information Services Security Policy (CJIS).
2. Agency shall ensure reasonable security of: physical security, including a secure area for placement of each item of TXGANG:
    a. equipment to preclude physical access by other than authorized personnel and to control visitor access;
    b. operational security, including TXGANG equipment operated to preclude system access by other than authorized personnel or for other than authorized purposes and to change system access.
    c. Identifiers for terminated or reassigned personnel; and
    d. personnel security, including access allowed only to:

    (1) Law enforcement or criminal justice personnel; or

    (2) Technical or maintenance personnel who have been subject to character or security clearance.
3. DPS may monitor the use of TXGANG by an agency through its User Agreement.
4. Compromising a user ID or password is a serious violation of system security.

AUDIT

1. Each Participating Agency is subject to a regular, triennial TCIC audit by a DPS representative. DPS may inquire into a demonstrated failure to comply with these policies and procedures.
3. A routine TCIC audit under these policies and procedures is an on-site:
    a) comparison of a random sampling of one or more TXGANG records submitted by the agency against its supporting documentation to ensure record and information quality; and
    b) review of system security measures and training records.
4. A Participating Agency will cooperate with each record review or audit of a TXGANG record.

SANCTIONS

1. If a Participating Agency materially violates any term of its User Agreement or these policies and procedures, the agency risks suspension of its access to TXGANG.
2. A suspension may occur immediately and without prior notice. Suspension may be followed by termination if deemed necessary by the Administrator.
3. The Administrator shall send to the Participating Agency a notice describing:
   a. the date the DPS has suspended or proposes to terminate service; and
   b. the alleged violation of the User Agreement.

TXGANG SYSTEM OPERATION

1. The Agency Administrator will be responsible for approving new users. After receiving FORM CSR-25G, the DPS will provide a user ID and password necessary for the new user to access the system through an authorized computer terminal. Passwords expire every 60 days. The authorized user must then create a new password.
2. The Agency Administrator must notify DPS when a user is terminated or reassigned and is, therefore, no longer eligible to continue as an authorized user.
3. Agency head and authorized users shall comply with DPS QC, Inspection, audit and validation procedures. Agency shall purchase, install, connect, configure and maintain equipment and software that it reasonably deems necessary for effective access to TXGANG; and is compatible with DPS specifications.
4. The agency head must ensure that each user with ***direct access*** to TXGANG is authorized, properly trained and using an appropriate electronic transmission. Agency head shall maintain an on-site list of current authorized users and submit the list to DPS.
5. Agency head shall designate at least one individual to serve as an authorized user and the agency's Primary Representative. Agency head must also designate one alternate representative. The agency head may self-designate as a primary, alternative or authorized user. Agency head may designate additional authorized users for the agencies and limit the

type of access allowed by the agency to certain individual users, including query-only access.

6. The Primary representative ensures compliance with policies and procedures and submits each required report or documentation. The Primary representative serves as first-level contact for DPS on TXGANG matters, audits and first-level support for questions from authorized users applications and equipment.
7. The Primary representative shall be the coordinator for TXGANG training within the agency.
8. Authorized Users-may query through direct access to TXGANG. Designated users must be qualified, trained and authorized under these policies and procedures and must be assigned to a clerical, administrative, technical, system maintenance or other support position under the administrative control of the agency; or regularly assigned to a unit that regularly investigates gang activity.
9. Un-authorized individuals may seek indirect access by making a personal telephone, electronic or other query of TXGANG through DPS or a participating agency ***AND*** demonstrating the individual's right and need to know.

DISSEMINATION

1. Agency must ensure that TXGANG records directly disseminated to authorized users include safeguards including a special user ID and initial password.
2. Agency shall only disseminate a record to a participating agency through a proper query by an authorized user from an authorized computer terminal.
3. All information maintained in the record will be released to an authorized user who makes a proper query, without any special restriction on its dissemination beyond the general requirements of 28 CFR.
4. TXGang creates an audit trail when it disseminates a TXGANG record, including the following information: the date and time of the query or other related transaction, the name of the individual requestor and the name of the agency requesting the record.
5. Agency shall create a dissemination log when the agency disseminates a TXGANG record. The log must comply with the principles of 28 CFR; and be

maintained for as long as the information supports a current TXGANG record.

6. Agency will permit indirect access to a TXGANG record by dissemination typically through a personal intervention; and using a communications network only if the network involves an encrypted radio broadcast or other reasonably secure transmission method, except in the case of an emergency, when necessary to avoid imminent danger to lie or property.
7. DPS will normally oppose a public information (open records) request for a TXGANG record based on CCP Ch. 67, the law enforcement exception, or another appropriate ground.

DATA ENTRY & QUALITY CONTROL

1. Agency must meet the entry criteria requirements to make an entry into TXGANG. Criminal Intelligence Information including facts, material, photographs or data must be evaluated to determine that it is relevant to the identification of an individual as a member of an organization for which a proper criminal predicate exists. (Gang and individual criteria listed in the handbook.)
2. Agency must determine Criminal Predicate exists based on articulable information and sufficient facts to give a trained criminal justice officer, investigator or employee reasonable suspicion to believe that a particular criminal street gang organization is or may be involved in definable criminal activity or enterprise.
3. Agency must ensure the quality of each record submitted to TXGANG as well as the quality of the information supporting that record.
4. Agency must maintain all supporting documentation for as long as the record is in TXGANG; or a legal challenge to the record is pending.
5. The entering agency is solely responsible for the quality of the information stored in a TXGANG record; and modifying or deleting a record if agency receives an order of expunction or if agency discovers it to be misleading, inaccurate, outdated or otherwise no longer relevant.
6. Agency at any time before the expiration of a TXGANG records current retention period may modify or delete a TXGANG record.
7. No one may submit or modify a TXGANG record unless a Participating Agency head has properly designated the individual as an authorized user on behalf of the agency.

8. If the agency knows it has new information supplementing one of its current TXGANG records, the agency must submit the information as a modification of its original record and may not create a second original record, unless the former record was juvenile and the proposed second record will be adult.
9. A Participating Agency that is subject to mandatory CCP Ch. 67 participation, must submit its information as a TXGANG record, even if the agency knows another Participating Agency has already established a TXGANG record on the same subject.
10. TXGANG prohibits a duplicate record on a single individual juvenile from a single Participating Agency; and adult from a single Participating Agency.
11. DPS does not prohibit duplicate TXGANG records from two or more agencies on the same gang member. A Participating Agency that is subject to mandatory CCP Ch. 67 participation, must submit its information as a TXGANG record, even if the agency knows another Participating Agency has already established a TXGANG record on the same subject.
12. When a TXGANG record is created based on certain alleged conduct of an individual, TXGang determines the individual's status as an adult or juvenile using the individual's age on the date of the conduct. TXGANG uses age on the date of the custody, not the date of submission, to determine the individual's status as a juvenile.
13. TXDPS uploads and updates each of the more than 48,000 unique TXGANG gang member records to the NCIC database. This creates an active NCIC Gang Member record and results in increased officer safety and situational awareness in the field. The data sent is *only* generated as an NCIC return in response to a Wanted Person inquiry, and is not available to search via TLETS as a gang investigative tool. However, investigative access remains available through the TXGANG database. All gang updates to the NCIC file are made via TXGANG – local law enforcement does not have to do additional entry once the records are entered into TXGANG. The NCIC Gang file and TXGANG have different criteria for entry, so not all records entered into TXGANG will be uploaded into NCIC.

RECORD VALIDATION

1. Agency record validation ensures that a TXGANG record continues to comply with both 28 CFR and the removal process described in CCP Ch. 67 (SB 418).
2. The DPS will only accept validation from the agency originally submitting the record.
3. At any time before the expiration of a TXGANG record's current retention period, a Participating Agency may validate the TXGANG record.
4. Validation should consist of reviewing of all documents, photographs, court documents, etc., to determine its relevance and validity. Review any supplemental information and verify retention.
5. Validation may include information asserting that an individual adult or juvenile gang member is not subject to removal under CCP Ch. 67 because the retention period contained one or more stated periods of time that should not be counted, including certain confinement or commitment; the adult subject of the file was arrested for criminal activity reported to DPS under Chapter 60, Code of Criminal Procedure; or the juvenile subject of the file was arrested for criminal activity reported to DPS under Chapter 60, Code of Criminal Procedure; or taken into custody for delinquent conduct reported to DPS under Chapter 58, Family Code.

RETENTION

1. The DPS will automatically remove from TXGANG any record that has passed its retention period without being validated under these policies and procedures. If an agency desires that the record be retained, it must validate it under the retention requirements of these policies and procedures.
2. When calculating the expiration of a retention period under CCP Ch. 67 (SB 418), TXGANG will not count any time period while the subject individual is confined in the institutional or state jail division of TDCJ; or committed to TYC for felony delinquent conduct; or confined in a county jail after conviction.
3. When calculating the expiration of a retention period, TXGANG will count any time period while the subject individual is under arrest or in custody of a peace officer; confined in a city jail, county jail, or other penal institution for pre-trial detention; or subject to probation or other form of community supervision.

4. The initial retention period for a record is five years after voluntary submission of a criminal street gang record not otherwise subject to CCP Ch. 67; three years after mandatory submission under CCP Ch. 67 of a record concerning an individual adult gang member; and two years after mandatory submission under CCP Ch. 67 of a record concerning an individual juvenile gang member.
5. The initial retention period for a TXGANG record is extended for a like period (five, three, or two years, respectively) after the date the information is validated under the retention requirements of these policies and procedures. A record's retention period is calculated from the later date of its original submission or its subsequent validation.
6. If a validation under CCP Ch. 67 is based on the individual being arrested or taken into custody, TXGANG uses the date of the arrest or custody, not the date of submission, to calculate any extension of the initial retention period. If a TXGANG record is later modified, TXGANG uses the initial date of the original record, not the date of modification, to calculate its initial retention period.
7. TXGANG will remove a record if the DPS receives an appropriate court order; determines the record to be misleading, inaccurate, outdated, or otherwise no longer relevant; or determines the submitting agency has failed or refused to provide adequate documentation of any material information supporting the record.

USE OF CHRI (CRIMINAL HISTORY RECORD INFORMATION)

1. TXGANG provides a live display of the gang member's rap sheet, based on the Texas SID provided and connecting directly to the Texas Computerized Criminal History files. Criminal history information obtained from the Texas CCH is confidential and subject to restrictions on the use and dissemination. Texas Government Code 411.085 provides the penalties for misuse of criminal history record information.
2. Additionally, the ultimate sanction available to TCIC management for enforcement of system policy is to discontinue system access to NCIC and TCIC criminal history record information.

STORAGE AND DESTRUCTION OF CHRI

1. When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.
2. CHRI shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

DISPOSAL OF ALL MEDIA

1. The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. (CJIS Security Policy 5.7 - 5.8.3 Digital Media Sanitization and Disposal)

2. Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel. (CJIS Security Policy 5.7 – 5.5.8.4 Disposal of Physical Media)