FORT WORTH INTELLIGENCE EXCHANGE (INTEX) - PRIVACY POLICY

I. PURPOSE STATEMENT

The FORT WORTH INTELLIGENCE EXCHANGE (INTEX) was established in response to the increased need for timely information sharing and exchange of crime and counterterrorism-related information and intelligence among members of the law enforcement, homeland security, and public safety communities. The Fort Worth INTEX will facilitate the collection, integration, evaluation, analysis, and dissemination of information and intelligence through established procedures for law enforcement, homeland security, and public safety purposes. The Fort Worth INTEX services are made available to law enforcement agencies and other entities contributing to homeland security and public safety throughout the Western portion of the Dallas/Fort Worth Metropolitan area, the State of Texas, and nationwide.

II. GOVERNANCE AND OVERSIGHT

A. Primary responsibility for the operation of the Fort Worth INTEX is assigned to the Fort Worth Police Department (FWPD). The INTEX's governance shall consist of an Advisory Board, Center Director, and Privacy Officer, each described below.

B. The Advisory Board shall be comprised of four sworn personnel, two civilian personnel, and one position open to sworn or civilian personnel from local agencies in the Fort Worth INTEX area of responsibility. The advisory board will be chaired by the Fort Worth INTEX director, or designee, who shall not have a vote except in case of a tie. The Privacy Officer shall be included in the board in a consultation role but shall not have a vote. One state and one federal representative or partner may be a member of the non-voting membership of the INTEX advisory board. The Advisory Board shall meet as needed and agreed upon by Board members. This Board shall assess the progress and processes of the Fort Worth INTEX and make recommendations to the Fort Worth INTEX chain of command on improvements or adjustments to better service the region. Implementation of these recommendation are at the discretion of the Fort Worth INTEX chain of command. Recommendations may be made on issues including, but not limited to:

a. Resolution of conflicts or disputes that may arise related to policy or mission;
b. Establishing or adjusting protocol concerning the treatment of violations of this Agreement;
c. Controlling the dissemination of any information produced by the Fort Worth INTEX including specific alerts and bulletins to agencies inside and outside the region;
d. Resolving disputes between FLO partners arising from the operation and activity of the Fort Worth INTEX, if not already addressed in the MOU;
e. Reviewing and updating the Fort Worth INTEX Privacy Policy annually based upon any changes in applicable law.
f. The board shall provide an annual report to the Fort Worth INTEX chain of command and the Fusion Liaison Officers on the status and efficacy of the Privacy Policy and the Fort Worth INTEX based upon any internal and external audits conducted.

C. The Fort Worth INTEX Director will be a Fort Worth Police Lieutenant assigned to the Intelligence Exchange Section. The Fort Worth INTEX Director will be responsible for the day to day operation of the Fort Worth INTEX. The Director will establish needed procedures, practices and protocols as well as use advanced software, information technology tools, and physical security measures to ensure information and intelligence are accessed only by authorized personnel and are protected from unauthorized access, modification, theft or sabotage, whether internal or external, or disasters or intrusions by natural or human causes. The Director shall coordinate with the Privacy Officer, described below, to ensure that enforcement procedures and sanctions as specified in this policy are adequate and enforced.

D. The Fort Worth INTEX shall have a trained Privacy Officer who is appointed by the Chief of Police consistent with the Fort Worth Police Department (FWPD) Integrated Information System (IIS) privacy policy and who assists the Advisory Board in investigating violations of this policy. The Privacy Officer shall receive and investigate reports of alleged errors in information and intelligence, coordinate error resolution under the center's redress policy, serve as the liaison for the Information Sharing Environment, and coordinate with other fusion centers in the State of Texas. The Privacy Officer shall coordinate with the Center Director to ensure adherence to enforcement procedures, and that such procedures are adequate. The Privacy Officer shall also review all analytical products to ensure that they provide appropriate privacy, civil rights, and civil liberties protections before dissemination or sharing by the center.

E. Individual users of the Fort Worth INTEX's information remain responsible for the lawful and appropriate use of the information and intelligence provided by the Fort Worth INTEX. Failure to abide by the restrictions and use limitations for Fort Worth INTEX's data may result in the suspension or termination of individual user privileges, disciplinary sanctions imposed by the user's employing agency, or criminal prosecution. Each user and agency participating in the Fort Worth INTEX is required to abide by this privacy policy in providing information and intelligence to the Fort Worth INTEX and in the access, use, security, and disclosure of information and intelligence obtained by and through the center.

III. Fort Worth INTEX Staffing and Organizational Structure

A. The Fort Worth INTEX is a collaboration of multiple full-time units working together to implement the mission of the center.

   a. Real-Time Crime Center: Tactical Information Officers working about 20 hours/day, 7 days/week. This unit provides real-time information and intelligence to patrol officers responding to calls for service. The RTCC also acts as an after-hours watch center for the fusion center.
   b. Criminal Intelligence Analyst Unit: Also known as the fusion unit, this unit is comprised of two criminal intelligence analysts, one counter-drug analyst, and two tactical information officers working in the Crime Stoppers program.
   c. Fort Worth Homeland Security Unit: This unit investigates threats to public safety, special events, protests, and dignitary visits to Fort Worth. The unit

includes the department's FBI Joint Terrorism Task Force TFO.

d. Crime Analysts: This unit includes crime analysts assigned to the Fort Worth Police divisions analyzing crime trends and data to assist commanders with resource allocation.

B. The Fort Worth INTEX includes the collaboration of multiple part-time personnel to assist with the mission of the center.

a. Fort Worth Fire Department: The Fort Worth Fire Department has provided a liaison from their Homeland Security Unit and a liaison from the Arson/Bomb unit to engage with the fusion center regularly.

b. Fort Worth Office of Emergency Management: The Fort Worth OEM has provided the ability for emergency managers to engage in the fusion center regularly to increase access to CIKR information and to progress the fusion center's capability for performing as an all-hazards/all-crimes center.

c. Fusion Liaison Officer Program: The Fort Worth INTEX will train fusion liaison officers from law enforcement agencies across the area of responsibility. These officers will act as points of contact for the sharing of information and intelligence throughout the region and will be capable of supplementing the staffing needs in the center.

d. Private Sector Outreach Program: Representatives from the private sector will be trained on how to share information and/or intelligence with the center to provide an overall situational awareness of crime trends and suspicious activity affecting the private sector.

IV. Fort Worth INTEX Collaboration

Fusion Liaison Officer Program- a collaborative effort between the Fort Worth INTEX and surrounding local jurisdiction to increase the information and intelligence flow throughout the region. It includes the integration of sworn and civilian criminal justice personnel from multiple jurisdictions into the INTEX operation under a Memorandum of Understanding.

Peer Fusion Center- another fusion center nationally recognized by the Department of Homeland Security that has goals, values, and a mission comparable to the Fort Worth INTEX, and that have adopted a Privacy Policy that is comparable to and as comprehensive as the Fort Worth INTEX Privacy Policy.

Private Sector Outreach Program- A collaborative effort between the Fort Worth INTEX and private sector representatives to increase information and intelligence sharing to identify crime trends and suspicious activity related to the private sector. The program will assist with debunking overhyped threats and providing the context to best server partners and their customers.

V. FWPD IIS PRIVACY POLICY

The Fort Worth INTEX information and intelligence privacy and protection is governed by the Fort Worth Police Department (FWPD) Integrated Information System (IIS) Privacy Policy included in this section and extends to the Fort Worth INTEX area of responsibility.

The privacy policy is as follows:

Section 1 - Purpose

A. The mission of the Fort Worth Police Department (FWPD) Integrated Information System (IIS) is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the FWPD area of responsibility while following appropriate privacy and civil liberties safeguards as outlined in the principles of the Organization for Economic Cooperation and Development's (OECD) Fair Information Principles to ensure that the information privacy and other legal rights of individuals and organizations are protected (see definitions of "Fair Information Principles" and "Protected Information" in Appendix A, Terms and Definitions).

B. The purpose of this privacy, civil rights, and civil liberties protection policy is to promote FWPD IIS and user conduct that complies with applicable federal, state, local, and tribal law (see Appendix A, Terms and Definitions) and assists FWPD in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the reluctance of individuals or groups to use or cooperate with the justice system.
- Supporting the role of the justice system in society.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening the ongoing business of the justice system.
- Making the most effective use of public resources allocated to public safety agencies.

Section 2 - Applicability and Legal Compliance

A. All FWPD IIS personnel, participating agency personnel, personnel providing information technology services to the system, private contractors, and other authorized users will comply with FWPD IIS's privacy policy. This policy applies to information the system gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to FWPD personnel, governmental agencies (including Information Sharing Environment (lSE) participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

B. The FWPD IIS will provide a printed or electronic copy of this policy to all FWPD and non-FWPD personnel who provide services and to participating agencies and individual users and will require both a written acknowledgment of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

C. All FWPD personnel, participating agency personnel, personnel providing information technology services to the FWPD IIS, private contractors, agencies from which FWPD IIS information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to 28 CFR Part 23, the National Criminal Intelligence Sharing Plan (NCISP), Texas Government Code, Title 5, Chapter 552.

D. The FWPD IIS has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to: Privacy Act of 1974, 28 CFR Part 23, the National Criminal Intelligence Sharing Plan (NCISP), and Texas Government Code, Title 5, Chapter 552.

Section 3 - Governance and Oversight

A. Primary responsibility for the operation of the FWPD IIS; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policyis assigned to the current Privacy Officer in the Program Support Division of the FWPD.

B. The FWPD IIS is guided by a designated privacy oversight committee that liaises with the community to ensure that privacy and civil rights are protected as provided in this policy and by the entity's information-gathering and collection, retention, and dissemination processes and procedures. The committee will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections. At a minimum, the oversight committee will include a member of the FWPD public relations office, a command level staff member of FWPD program support division, and a designee from the Chief of Police.

C. FWPD's privacy committee is guided by a trained Privacy Officer, who is appointedby the Chief of Police. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the entity's redress policy (see Section 11 of this policy), and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: Fort Worth Police, Program Support Division, Privacy Officer, 505 West Felix St., Fort Worth, TX 76115.

D. The Privacy Officer ensures that enforcement procedures and sanctionsoutlined in Section 14.3, Enforcement, of this policy are adequate and enforced.

Section 4 - Definitions

A. Primary terms and definitions used in this policy are included in Appendix A - Terms and Definitions.

Section 5 - Information

A. The FWPD IIS will seek or retain information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
- Is applicable to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Is useful in criminal intelligence analysis or the administration of criminal justice and public safety (including topical searches), and
- The source of information is reliable and verifiable, or limitations on the quality of the information are identified, and
- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

The FWPD IIS may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

B. The FWPD IIS will not seek or retain and information-originating entities will agree not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

C. The FWPD IIS applies labels to FWPD-originated information (or ensures that the originating entity has applied labels) to indicate to the accessing authorized user that:

- The information is "protected information," to include "personal data" on any individual (see Appendix A - Terms and Definitions), and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to the state and federal laws outlined in Appendix B restricting access, use, or disclosure.

D. The FWPD IIS personnel will, upon receipt of information, assess the data to determine or review its nature, usability, and quality. Staff will assign categories to the information (or ensure that the originating entity has assigned categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, an anonymous tip, trained interviewer or investigator, public record, private sector).

- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

E. At the time a decision is made by the FWPD IIS to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right to privacy or his or her civil rights and civil liberties.
- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

F. The labels assigned to existing information under Section 5.E above will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

G. FWPD IIS personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips, leads, suspicious activity report (SAR) information, and Field Interview (FI) Cards. IIS personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The entity will use a standard reporting format and data collection codes for SAR information.
- Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an inter-entity inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for no more than six months to work an un-validated tip, lead, SAR information, or FI Card to determine its credibility and value or assign a

"disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

- Adhere to and follow the FWPD IIS physical, administrative, and technical security measures to ensure the protection and security of tips, leads, SAR information, and FI Cards. Tips, leads, SAR information, and FI Cards will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

H. The FWPD IIS incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

I. FWPD IIS will identify and review protected information that may be accessed from or disseminated by FWPD before sharing that information through the Information Sharing Environment. Further, FWPD will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

J. FWPD IIS requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

- The name of the originating entity, department or entity, component, and subcomponent.
- The name of the entity's justice information system from which the information is disseminated.
- The date the information was collected and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

K. FWPD IIS will attach (or ensure that the originating entity has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

L. FWPD IIS will keep a record of the source of all information sought and collected by the FWPD IIS.

Section 6 - Acquiring and Receiving Information

A. Information-gathering (acquisition) and access and investigative techniques used by the FWPD IIS and information-originating entities will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

- Referenced laws are listed in appendix B
- 28 CFR Part 23 regarding criminal intelligence information.
- The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or FWPD policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Constitutional provisions; Texas Government Code, Title 5 Chapter 552; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

B. The FWPD IIS SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate entity and participating entity staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

C. The FWPD IIS SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals and organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.), and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

D. Information-gathering and investigative techniques used by the IIS will, and those used by originating entities should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

E. External entities that access or share information with the FWPD IIS will provide an assurance in future contracts (i.e., within interagency agreements, MOUs, etc.) that they comply with laws and rules governing those individual entities, including applicable federal and state laws. Furthermore, FWPD IIS will attempt to amend current Agreements to reflect this compliance.

F. The FWPD IIS will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices, unless deemed necessary by the FWPD Chief of Police.

G. The FWPD IIS will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or entity policy.
- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

Section 7 - Information Quality Assurance

A. The FWPD IIS will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard (see Section 9, Merging Records) has been met.

B. At the time of retention in the system, the information will be labeled regarding its level of currency, validity and reliability.

C. FWPD IIS investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating entity) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

D. The labeling of retained information will be reevaluated by FWPD IIS or the originating entity when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

E. FWPD IIS will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the entity identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the entity did not have the authority to gather the information or to provide the information to another entity; or the entity used prohibited means to gather the information (except when the entity's information source did not act as the agent of the entity in gathering the information).

F. Originating entities external to FWPD are responsible for reviewing the quality and accuracy of the data provided to FWPD. FWPD IIS will review the quality of information it has received from an originating entity and advise the appropriate contact person in the originating entity, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

G. FWPD IIS will use written or electronic notification to inform recipient entities when information previously provided to the recipient entity is deleted or changed by FWPD IIS because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

Section 8 - Collation and Analysis

A. Information acquired or received by the FWPD IIS or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

B. Information subject to collation and analysis is information as defined and identified in this policy (see Section 5 -Information).

C. Information acquired or received by the FWPD IIS or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

- Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the entity.
- Provide tactical and strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

D. FWPD IIS requires that all analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections.

Section 9 - Merging Records

A. Information will be merged only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

B. Records about an individual or organization from two or more sources will not be merged by the FWPD IIS unless there is sufficient identifying information to clearly establish that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of the match.

C. If the matching requirements are not fully met, but there is a reason to believe the records are about the same individual, the information may be associated by FWPD IIS if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

Section 10 - Sharing and Disclosure

A. Credentialed, role-based access criteria will be used by the FWPD IIS, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under whatcircumstances.

B. FWPD IIS adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format, commonly accepted data collection codes, and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

C. Access to or disclosure of records retained by the FWPD IIS will be provided only to persons employed with FWPD or in other governmental entities who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the entity for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the IIS and the nature of the information accessed will be kept by FWPD (see F. below for exceptions).

D. Entities external to the FWPD may not disseminate information accessed or disseminated from the IIS without approval from FWPD or other originators of the information.

E. Records retained by the IIS may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties following applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the IIS and the nature of the information accessed will be kept by FWPD.

F. Information gathered or collected and records retained by the IIS may be accessed or disclosed to a member of the public only if the information is defined by law (Title 5 of the Texas Government Code) to be a public record or otherwise appropriate for release to further the entity's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the entity for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the entity and the nature of the information accessed will be kept by the entity as required by law, but may only be disclosed in connection to a challenge to the legitimacy of the disclosure itself but not for investigatory or other criminal justice purposes.

G. Information gathered or collected and records retained by the FWPD IIS may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the IIS; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of two years.

H. Information gathered or collected and records retained by the IIS will not be:
- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication unless disclosure is agreed to as part of the normal operations of the entity.
- Disseminated to persons without a legal right to know the information.

I. There are several categories of records that will ordinarily not be provided to the public, including but not limited to:
- Records required to be kept confidential by law are exempted from disclosure requirements under the Texas Government Code, Title 5, Chapter 552.
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Investigatory records of law enforcement entities that are exempted from disclosure requirements under Texas Government Code, Title 5, Chapter 552.
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments. These are exempted from disclosure requirements under Texas Government Code, Title 5, Chapter 552.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another entity that cannot, under Texas Government Code, Title 5, Chapter 552, be shared without permission.
- A violation of an authorized nondisclosure agreement under Texas Government Code, Title 5, Chapter 552.

J. FWPD shall not confirm the existence or nonexistence of information to any person or entity that would not be eligible to receive the information unless otherwise required by law.

Section 11 - Redress Section

11.1- Disclosure

A. Response to written requests for information will be made within 10 days of the request, in a form that is readily intelligible to the individual, and in compliance with Texas Government Code, Title 5, Chapter 552. A record will be kept of all requests and of what information is disclosed to an individual for two years.

B. The existence, content, and source of information will not be made available by FWPD to an individual when exempted from release under the Texas Government Code, Title 5, Chapter 552 and a request for an opinion is sent to the Texas Attorney General for a determination that:
- Disclosure would interfere with, compromise, or delay an ongoing investigation or

prosecution. *See* Texas Government Code, Section 552.108.
- Disclosure would endanger the health or safety of an individual, organization, or community. *See* Texas Government Code, Sections 418.176 and 552.108(b)(1).
- The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].
- The information source does not reside with FWPD IIS.
- FWPD IIS did not originate and did not have a right to disclose the information.
- Other authorized basis for denial.

If the information does not originate with FWPD, the requestor will be referred to the originating entity, if appropriate or required, or FWPD will notify the source entity of the request and its determination that disclosure by FWPD or referral of the requestor to the source entity was neither required nor appropriate under applicable law.

Section 11.2 - Corrections

A. If an individual requests correction of information originating with FWPD IIS that has been disclosed, the Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action if any.

B. Appeals will be referred to as the privacy oversight committee.

Section 11.3 - Appeals

A. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by FWPD or the originating entity. The individual will also be informed of the procedure for appeal when the FWPD or originating entity has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates. All appeals will be handled in accordance with Texas Government Code, Title 5, Chapter 552.

Section 11.4 - Complaints

A. If an individual has a complaint about the accuracy or completeness of terrorism-related protected information that:
(1) Is exempt from disclosure,
(2) Has been or may be shared through the ISE,
(3) Is held by FWPD IIS, and
(4) Allegedly has resulted in demonstrable harm to the complainant,

FWPD IIS will inform the individual of the procedure for submitting (if needed) and resolving such complaints.

Complaints will be received by the Privacy Officer (or designee) at the following address: Fort Worth Police Department, Program Support Division, Privacy Officer, 505 West Felix St., Fort Worth, TX 76115. The Privacy Officer (or designee) will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with FWPD, the Privacy Officer (or designee) will notify the originating entity in writing or electronically within ten days and, upon request, assist such entity in correcting any identified data/record deficiencies, purging the information, or verifying that the record is accurate. All information held by FWPD that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the entity will not share the information until the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to the complaint.

B. To delineate protected information shared through the ISE from other data, the IIS maintains records of entities sharing terrorism-related information and employs system mechanisms to identify the originating entity when the information is shared.

Section 12 - Security Safeguards

A. FWPD employs a designated and trained security officer.

B. FWPD IIS will operate in a secure facility protected from external intrusion. The entity will utilize secure internal and external safeguards against network intrusions. Access to the entity's databases from outside the facility will be allowed only over secure networks.

C. FWPD IIS will secure tips, leads, SAR information, and FI Cards in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

D. FWPD IIS will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

E. Access to the IIS will be granted only to entity personnel whose positions, and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

F. Queries made to the IIS data applications will be logged into the data system identifying the user initiating the query.

G. FWPD will utilize watch logs to maintain audit trails of requested and disseminated information.

H. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

I. FWPD IIS will follow the data breach notification specified in Texas Business and Commerce Code Section 521.053, to the extent that it applies. FWPD will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of the information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

Section 13 - Retention and Destruction

A. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23.

B. When information has no further value or meets the criteria for removal according to the FWPD retention and destruction policy, or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) entity.

C. FWPD will delete information or return it to the originating entity once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating entity in a participation or membership agreement.

D. No approval will be required from the originating entity before information held by FWPD IIS is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating entity in a participation or membership agreement.

E. Notification of proposed destruction or return of records may or may not be provided to the originating entity, depending on the relevance of the information and any agreement with the originating entity.

F. A record of information to be reviewed for retention will be maintained, and for appropriate system(s), notice will be given to the submitter at least 30 days before the required review and validation/purge date.

G. A printed or electronic confirmation of the deletion will be provided to the originating entity, where required under law or if part of the terms of a pre-established agreement with the entity.

Section 14 - Accountability and Enforcement

Section 14.1- System Transparency

A. FWPD will be open with the public regarding information and intelligence collection practices. The entity's privacy policy will be provided to the public for review, made available upon request, and posted on the entity's Web site at www.FortWorthPD.com.

B. The Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by FWPD. The Privacy Officer can be contacted at Fort Worth Police Department, Program Support Division, Privacy Officer, 505 West Felix St., Fort Worth, TX 76115.

Section 14.2 - Accountability

A. The audit log of queries made to the FWPD IIS will identify the user was initiating the query.

B. FWPD will maintain an audit trail of accessed, requested or disseminated information. An audit trail will be kept for a minimum of two years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

C. FWPD will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, to not establish a pattern of the audits. These audits will be mandated at least annually, and a record of the audits will be maintained by the Privacy Officer.

D. FWPD IIS personnel or other authorized users shall report errors and suspected or confirmed violations of entity policies relating to protected information to the Privacy Officer (see Section 3C of this policy).

E. FWPD will annually conduct an audit and inspection of the information and intelligence contained in the IIS. The audit will be conducted by the Privacy Officer, who has the option of conducting a random audit, without announcement, at any time and without prior notice to staff. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the IIS.

F. A privacy committee, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

Section 14.3 - Enforcement

A. If FWPD personnel, a participating entity, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Chief of Police of FWPD will:

- Suspend or discontinue access to information by the authorized user.
- Suspend, demote, transfer, or terminate FWPD personnel, as permitted by applicable personnel policies, in accordance with Texas Local Government Code, and as permitted by existing City of Fort Worth agreements.
- Apply administrative actions or sanctions as provided by FWPD rules and regulations or as provided in FWPD personnel policies, and in accordance with Texas Local Government Code.
- If the authorized user is from an entity external to FWPD, request that the relevant entity, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

B. FWPD reserves the right to restrict the qualifications and number of personnel having access to the IIS and to suspend or withhold service and deny access to any participating entity or participating entity personnel violating this policy.

Section 15 - Training

A. FWPD will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

- All assigned personnel of the FWPD Program Support Division.
- Personnel providing information technology services to FWPD.
- Users permitted to access the FWPD IIS who are not employed by FWPD or a contractor.

B. FWPD will provide special training regarding the entity's requirements and policies for the collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

C. The privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by FWPD.
- Originating and participating entity responsibilities and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
- The impact of improper activities associated with infractions within or through FWPD.

- Mechanisms for reporting violations of privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A - Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the center's privacy policy.

Access-Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control-The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition-The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Audit Trail-A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail-what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Civil liberties-Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights-the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights-The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and

by acts of Congress.

Computer Security-The protection of information assets through the use of technology, processes, and training.

Confidentiality-Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials-Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information-Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data-Inert symbols, signs, descriptions, or measures; elements ofinformation.

Data Breach-The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media including computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection-Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure-The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner-electronic, verbal, or in writing-to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained-Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted-Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extra net, leased lines, dialup

lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left onvoicemail.

Fair Information Principles-The Fair Information Principles (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justicesystems.
Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:
- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

General Information or Data-Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information-As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terroristact.

Identification-A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Information-Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, including investigative

information; tips and leads data; suspicious activity reports; and criminal intelligence information.

Information Quality-Refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (lSE-SAR)-A
SAR that has been determined, under a two-step process established in the ISE- SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Integrated Information System (IIS)-the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information, and is governed by the Code of Federal Regulations, 28 CFR Part 23.

Law-As used by this policy; law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information-For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident-A foreign national who has been granted the privilege of permanently living and working in the United States.

Logs-A necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Metadata-In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of

metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know-As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

Originating Agency-The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Participating Agency-An organizational entity that is authorized to access or receive and use center information and intelligence databases and resources for lawful purposes through its authorized individual users.

Permissions-Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information-Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

Personally Identifiable Information-One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, drivers license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).
- Descriptions of the event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons-Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an

unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy-Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy-A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well- developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the center, the individual, and the public; and promotes public trust.

Privacy Protection-A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information-protected information includes Personal Information about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Texas constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or another state, local, or tribal agency policy or regulation.

Public-Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the center's information.
- Media organizations.
- Entities that seek receive or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the center or participating agency. The public does not include:
- Employees of the center or participating agency.
- People or entities, private or governmental, who assist the center in the operation of the justice information system.

- Public agencies whose authority to access information gathered and retained by the center is specified in the law.

Public Access-Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Record-Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress-Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Retention-Refer to Storage.

Right to Know-Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of law enforcement, homeland security, or counterterrorism activity.

Right to Privacy-The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access-A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic categoryof users that share the same security privilege.

Security-Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency-Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

Storage-In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages: Storage is frequently used to mean the devices and data connected to the computer through input/output operations-that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the

most common meaning in the IT industry. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's II cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage. With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information-including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland-by both the originator of the information and any recipient of the information.

Suspicious Activity-Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)-Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information, FI Card analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information, FI Card is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information-Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information-In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3,2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.c. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information"; (1) homeland security information as defined in Section 892(f)(1) of the

Homeland Security Act of 2002 (6 U.S.c. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information. Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Tips and Leads Information or Data-Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as asuspicious incident report (SIR), suspicious activity report (SAR), and field interview report (FIR) information. However, SAR information and FI Card should be viewed, at most, as a subcategory of the tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion. A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User-An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

Appendix B
Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Following is a partial listing of state and federal laws arranged in alphabetical order by popular name.

Texas Laws
Texas Government Code, Title 5, Chapter 552 Texas
Government Code, Section 552.108
Texas Government Code, Sections 418.176 and 552.108(b)(1) Texas
Business and Commerce Code Section 521.053

Federal Laws
Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-Ol-05, "Guidance on Interagency Sharing of Personal Data Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22,

Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal lntelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title
28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522,2701-2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510-2522, 2701-2709, and3121-3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301
Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968,25 U.S.C. § 1301, United States Code, Title 25,Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993),107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code ofFederal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272