Houston Regional Intelligence Service Center (Fusion Center) Privacy Policy

---

Privacy, Civil Rights, and Civil Liberties Policy

Contents

Houston Regional Intelligence Service Center
Privacy Policy

I. Purpose

1. The Houston Regional Intelligence Service Center is a Fusion Center (hereafter referred to as the "Center") as defined below:

2. The Houston Regional Intelligence Service Center is a Houston Police Department (HPD) led effort and has primary responsibility for the Center, (justice systems, operations and enforcement of policies). Violation of its policies will be addressed jointly by HPD and participating agencies. Daily group supervision and direction is the responsibility of the sergeant assigned to the Center from the Houston Police Department. Participating collocated members will bring to the attention of the Center's group supervisor any protocol or action which is not in compliance with that member's agency's rules or operating protocols or violations of HRISC policies, so that it may be immediately addressed.

3. The mission of the Houston Regional Intelligence Service Center (Center) is to provide continuous security to our region by gathering, developing and sharing intelligence into the capabilities, intentions, and actions of terrorist groups and individuals which pose a threat to our populace and region.

4. The Fusion Center project was initiated in response to the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of the Center focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

5. The Center's intelligence products and services will be made available to law enforcement agencies and other criminal justice entities in accordance with the provisions of this policy. All collocated agencies participating in the Center will be subject to a Memorandum of Understanding and will be required to adhere to all Center policies, security requirements and this privacy policy. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged.

6. The desired outcome of this policy is to ensure that the rights of all citizens under the Constitution of the United States are protected.

7. This *Privacy Policy* embraces the eight Privacy Design Principles that include the following:

(a) Purpose Specification - All Houston Regional Intelligence Service Center (HRISC) personnel will comply with the Houston Regional Intelligence Service Center's privacy policy concerning the information the Center collects, receives, maintains, archives, accesses, or discloses to ensure the rights of all citizens are protected**.**

(b) Collection Limitation - All information and intelligence will be obtained lawfully and products produced will be handled in accordance with 28 CFR Part 23, and applicable State of Texas laws.

(c) Data Quality - The Center will make every reasonable effort to seek information from dependable and trustworthy sources and that it is accurate, current, complete, valid and reliable, including relevant content.

(d) Use Limitation - Access to or disclosure of records or information retained by the Houston Regional Intelligence Service Center will only be provided to persons who are authorized to have access and only for legitimate law enforcement, public safety, and criminal justice purposes, and only for the performance of official duties in accordance with law and procedures.

(e) Security Safeguards - The Center's supervisor and a designated security officer, who shall receive appropriate training, will serve as the Houston Regional Intelligence Service Center security officers. The Center will operate in a secure facility protecting the facility from external intrusion. The Houston Regional Intelligence Service Center will utilize secure internal and external safeguards against network intrusions. The Center will store information in a manner such that it cannot be added to, accessed, destroyed, or purged except by personnel authorized to take such actions. Access to Houston Regional Intelligence Service Center databases from outside the facility will only be allowed over secure networks. Finally, the security of the Center in general is all members' responsibility. Violations of the Center's policies will be jointly resolved between the participating agencies and the Houston Police Department.

(f) Openness - Promote a general policy of openness about agency practices and policies regarding personal information.

(g) Individual Participation - Allow individuals reasonable opportunity to correct errors in their personal information held by the agency.

(h) Accountability - Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. All members of the Center will be given a copy of the privacy policy and collocated members will undergo privacy training**.**

8. The Center has developed databases by using existing data sources from participating entities to integrate data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information between the participating agencies.

II. <u>Collection Limitation</u>

1. The Center is maintained for the purpose of developing information and intelligence by agencies participating for the security of the region. The decision of the agencies to participate in the Center and which databases to provide is voluntary and will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable Texas State and federal laws.

2. The Center has adopted this privacy policy that all HRISC personnel and collocated members (center personnel) will be instructed on and must agree in writing that they will follow it. This policy and the Center's Operating Protocols are in compliance with the following applicable laws and regulations protecting privacy, civil rights, and civil liberties:

- 28 CFR part 23; the principle of need to know, right to know
- The Texas Crime Information Center and the National Crime Information Center compliant, Criminal Justice Information Systems compliant
- Texas Government Code 411.083 Dissemination of Criminal History Record Information; 411.084 Use of Criminal History Record Information; 411.085 Unauthorized Obtaining, Use, or Disclosure of Criminal History Record Information; Penalty.
- Texas Government Code, Chapter 552, Pubic Information Act
- Code of Federal Regulations, Title 28--Judicial Administration, Chapter I--Department of Justice, part 20--Criminal Justice Information Systems, Subpart A--General Provisions
- Texas and U.S. Constitutions

3. The Houston Police Department has oversight and is responsible for this privacy policy. The HPD sergeant who is the day to day supervisor of the Center will: serve as the Center's privacy official responsible for handling reported errors and violations in data; be responsible for receiving and responding to inquiries and complaints from the public concerning privacy, civil rights, and civil liberties protections in the Center's information system; ensure that all ISE requirements for handling terrorism-related information are adhered to; and be responsible for training personnel and compliance of this policy and all policies of the Center. Training will include this privacy policy, operating protocols and SAR training.

4. Vendors with access to Criminal Justice Information will have to comply with the rules set forth in the above mentioned laws and sign a security addendum for the protection of information.

5. The Center will seek or retain information which a source agency (the FC or other agency) has determined constitutes "suspicious activity," and which:

- Is based on (a) or suspected criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct.
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime.
- The source agency assures was acquired in accordance with agency policy and in a lawful manner.

6. The Center will label information it receives and shares as Law Enforcement Sensitive, For Official Use Only, Not For Public Release, etc.: label it to indicate whether it is subject to any legal restrictions on access, use, or disclosure; and ensure that basic descriptive information is entered into and electronically associated with the data, including the name of the originating agency, the date of submission, and the identity of the submitter. The classification and labeling

of existing information will be reevaluated whenever new information impacts the classification, including confidence (validity and reliability) or there is a change in the use of the information affecting access of disclosure limitations. Information will be identified as falling into various categories (inquires, tips and leads, SARs, offense reports, intelligence file). All SAR data, Inquiries, including tips and leads that are in the SAR database will be kept in that database for a period of one year, unless there is reasonable suspicion of criminal activity, in which they can be retained for up to 5 years.

7. Protected information (information that identifies or may be used to identify a specific individual or organization suspected of involvement in criminal activity) will only be released to law enforcement personnel, and terrorism-related SAR (ISE-SAR) information in the shared space environment will have been subject to initial inquiry or investigation to validate or refute the information and will be labeled as to its sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and appropriately categorized, with source citations notated where applicable. With analytical products, the officers and analyst observations and opinions will be notated as theirs.

8. Information that is developed into an Intelligence file will be kept in accordance with the Criminal Intelligence Division's SOP 200-1.08 entitled "Organized Crime Files", and 28 CFR Part 23 and other applicable laws. This policy governs the process for maintaining and purging certain records (See page 3, #2).

9. Source agencies will agree not to collect and submit SAR information that was gathered solely on the basis of an individual's religious, political, or social views or activities; participation in a particular non-criminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

10. All SAR information will be processed and undergo a two step assessment as set forth in the ISE-SAR Functional Standard *Suspicious Activity Reporting (SAR) Version 1.5* (ISE-FS-200), to determine if it meets the criteria for placement in the shared space. The Center will secure SAR information in a separate repository system and adhere to the FS and established policies for ISE-SAR information under the ISE-SAR Evaluation Environment Initiative.

11. The Center will not tolerate or condone illegal activity or non-compliance regarding the appropriate federal laws/regulations or Texas law in the handling of information.

III. Data Quality

1. The agencies participating in the Center remain the owners of the data contributed to the Center and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the Center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated *before* any official action (e.g., warrant or

arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

2. Information coming into the Center regarding persons, activities, investigations, and operations will be treated as private, confidential, and law enforcement sensitive. The topic or subject under an intelligence inquiry will not be openly discussed with or near those who do not have the appropriate clearance or a *need to know, right to know.*

3. Subjects, topics, inquiries, information and intelligence products will be gathered, processed, and disseminated in strict accordance with 28CFR part 23; the principle of *need to know, right to know* will be strictly adhered to. The Center will conduct inquiries to determine the accuracy of some of the information it receives, and some information will be forward to the Joint Terrorism Task Force for vetting through that task force. Information placed in intelligence files will always be labeled for its reliability and validity as it applies to the source of the information and the information itself. Intelligence and SAR/ISE-SAR files will be strictly controlled, kept separate and apart, and will not be merged into other reports, files, and documents and will not be discussed unless there is a need to know or right to know. Source agency data will not be merged by the Center. Secret information will be shared with those with the appropriate clearance and who possess a strict need to know, right to know.

4. The Center will refer alleged errors or deficiencies in data to the originating agency, in writing, and refrain from using or sharing the data until it is validated or corrected by the source agency. When data is confirmed as erroneous, misleading, obsolete, or otherwise unreliable; the source agency did not have authority to gather the data or provide it to the Center; or the source agency used prohibited means to gather the data, the data will be purged. In addition, if the dissemination of the information may affect the rights of an individual, all agencies that have received the information will be notified and requested to purge the information from their files.

5. Destruction of data created by the Center will be in accordance with City of Houston record retention policies (city ordinance 2-111), Article 6252-17a, Vernon's Texas Civil Statutes, 28 CFR Part 23, and incompliance with the Texas State Library and Archives Commission.

IV. Use Limitation

1. Information obtained from or through the Center will only be used for lawful purposes. A lawful purpose includes the following: the request for data can be directly linked to a law enforcement agency's active criminal investigation, the request for data is a response to a confirmed lead that requires follow-up to prevent a criminal act or to aid in apprehension, there is reasonable suspicion to believe that the subject is possibly involved in criminal activity or there is reasonable suspicion that the group or subject could pose a threat to the community.

2. Primary responsibility for the operation of the Houston Regional Intelligence Service Center, its justice systems, operations, coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Houston Police Department and participating agencies of the Houston Regional Intelligence Service Center.

3. Security for information derived from the Center will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who work in the Center who receive, handle, or have access to Center data and/or sensitive information including ISE information, will be trained in this policy and given a copy of those operating protocols. All personnel in the Center agree to abide by the following rules:

- The Center's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.
- Individual passwords will not be disclosed to any other person except as authorized by agency management.
- Individual passwords will be changed if authorized personnel of the agency or members of the Center suspect the password has been improperly disclosed or otherwise compromised.
- Background checks will be completed on personnel who will have direct access to the Center.
- Use of the Center's data in an unauthorized or illegal manner will subject the user to denial of further use of the Center, discipline by the user's employing agency, and/or criminal prosecution.

4. Each authorized user understands that access to the Center can be denied or rescinded for failure to comply with the applicable restrictions and use limitations. All collocated personnel will be vetted at the "Law Enforcement Sensitive," and "Secret" level and will handle and distribute information as per the distribution caveat.

5. Information will be analyzed only by qualified personnel who have successfully completed a background check and any required security clearance and who have been selected, approved, and trained. Information will be analyzed to further crime prevention, enforcement, deployment, or prosecution objectives in accordance with priorities established by the Center and to provide tactical and/or strategic intelligence products.

V. Security Safeguards

1. Information obtained from or through the Center will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each collocated participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

2. Use of the Center's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the Center will be granted only to law enforcement agency personnel and homeland security personnel with a need to know right to know standard and who have been screened. Each collocated member must complete an Individual User Agreement in conjunction with training and policies. The Center will adopt and follow procedures and practices to ensure compliance of system users with this policy and

applicable law. This will include logging access to systems and periodic and random system audits.

3. Access to the Center's databases from outside of the Center will only be allowed over secure network lines and will identify the user initiating the query through the Center's audit log of queries to the system.

4. To prevent public records disclosure, risk and vulnerability assessments will not be stored in information file with any other data.

5. In the event of a data security breech, the Center will contact the appropriate prosecutorial authority and take other notification action that is deemed appropriate.

VI. Openness

1. It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities or active inquiry. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation. The Center will not release any information to the public, except as required under the Texas Public Information Act, Texas Government Code, Chapter 552. Complaints and requests for corrections will be referred to the appropriate agency or handled in accordance with HPD policy.

2. The Center will make this *Privacy Policy* available for public review when requested.

VII. Individual Participation

1. The data maintained by the Center is provided, on a voluntary basis, by the participating agencies or is information obtained from other sources by the Center. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination, and use of any information that results from the search process and is responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

2. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question.

3. The Center and participating agencies will refer requests related to disclosure of information or to privacy or sunshine laws back to the originator of the information for appropriate response. A record will be kept of all requests for information and referrals to source agencies. The Center will not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

4. If an individual has complaints or objections to the accuracy or completeness of protected information that is ISE information (terrorism-related), the Center's privacy official will notify the originating agency of the complaint and coordinate with them to ensure that the information is validated or, if erroneous or misleading, is corrected or purged in a timely manner. To delineate protected information shared through the ISE from other data, the Center maintains records, audit logs, and other system mechanisms to identify the source agency for all information maintained by the Center.

VIII. Accountability

1. When information is disseminated outside of the Center dissemination logs must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Requested information will also be noted on a log. This record will reflect at a minimum:

1. Date of release
2. Data released
3. To whom the information was released
4. The purpose for which the information was released
5. The name of the person who released the information

2. Access to or disclosure of records or information retained by the Houston Regional Intelligence Service Center will only be provided to persons who are authorized to have access for legitimate law enforcement, public safety, and criminal justice purposes, and only for the performance of official duties in accordance with law and procedures.

3. When no longer useful, all documents, drafts, copies of documents, email hard copies, and other items will be purged as per policy and shredded in the high security shredder and not placed in the black waste cans. Inspection of the logs will be conducted randomly.

4. The Security of the Fusion Center is everyone's responsibility and violations will be investigated by the HPD group supervisor or appropriate entity. Failure to abide by the restrictions and use limitations regarding the Center's data may result in the suspension or termination of use privileges, individual sanctions imposed by the user's employing agency, or criminal prosecution.

5. Each collocated participating agency in the Center will be trained in, and is required to abide by, this *Privacy Policy* in the purpose of the policy, its substance and intent, including the use, storage, and disclosure of information obtained by and through the Center, and how to implement the policy in the day-to-day work of the user. This privacy policy will be updated and reviewed as laws or procedures are changed. Audits regarding these procedures will be conducted by the Houston Police Department as per departmental procedure.

APPENDIX A
Terms and Definitions

Center—Center refers to the Houston Regional Intelligence Service Center.

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.

Civil Liberties—Civil liberties are 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 and 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.

Criminal Intelligence Information or Data—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 acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Logs—Logs are 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.

Privacy Policy—A privacy policy is a written, 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 agency/center will adhere to those legal requirements and agency/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 agency, the individual, and the public; and promotes public trust.

Suspicious Activity—Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR) Information—The observation and documentation of a suspicious activity. At the federal level, there are two types of SAR information: 1) Information Sharing Environment SAR information that pertains to terrorism information; and 2) Banking Secrecy Act SAR information that pertains to suspicious banking activity and is required to be completed by financial institutions. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

APPENDIX B
Relevant Federal and State Laws

- 28 CFR part 23; the principle of need to know, right to know
- The Texas Crime Information Center and the National Crime Information Center compliant, Criminal Justice Information Systems compliant
- Texas Government Code 411.083 Dissemination of Criminal History Record Information; 411.084 Use of Criminal History Record Information; 411.085 Unauthorized Obtaining, Use, or Disclosure of Criminal History Record Information; Penalty.
- Texas Government Code, Chapter 552, Pubic Information Act
- Code of Federal Regulations, Title 28--Judicial Administration, Chapter I--Department of Justice, part 20--Criminal Justice Information Systems, Subpart A--General Provisions