AUSTIN REGIONAL INTELLIGENCE CENTER - PRIVACY POLICY

I. PURPOSE STATEMENT

The AUSTIN REGIONAL INTELLIGENCE CENTER (ARIC) 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 ARIC 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 ARIC services are made available to law enforcement agencies and other entities contributing to homeland security and public safety throughout the Austin-Round Rock metropolitan area, the State of Texas, and nationwide.

The goal of the Center is to further the following purposes:

(1) Increase public safety and improve national security
(2) Minimize the threat and risk of injury to specific individuals
(3) Minimize the threat and risk of damage to real or personal property;
(4) Protect individual privacy, civil rights, civil liberties, and other protected interests;
(5) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
(6) Minimize reluctance of individuals or groups to use or cooperate with the justice system;
(7) Support the role of the justice system in society;
(8) Promote governmental legitimacy and accountability;
(9) Not unduly burden the ongoing business of the justice system; and
(10) Make the most effective use of public resources allocated to justice agencies.

The purpose of this Privacy Policy is to ensure that safeguards and sanctions are in place to protect the privacy, civil rights and civil liberties of all individuals, and other protected interests, including those of organizational entities, as well as to protect the integrity of criminal intelligence investigations and justice system processes. It is also the purpose of this Policy to ensure accuracy of information and intelligence and compliance with applicable law as information and intelligence are developed, collected and exchanged.

The ARIC Privacy Policy incorporates the principles of the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA) as well as the Department of Justice's (DOJ) Global Justice Information Sharing Initiative.

II. DEFINITIONS

Criminal Intelligence System means 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.

Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

Intelligence is the product of an analytical process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality.

Information Sharing Environment-Suspicious Activity Report (ISE-SAR) is a SAR (defined below) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR information is governed by the Information Sharing Environment Functional Standard Suspicious Activity Reporting Version 1.5 (ISE-FS-200).

ARIC Interlocal Agreement (Interlocal Agreement) is the agreement between the Partner Agencies through their governmental entities, pursuant to the Interlocal Cooperation Act (Texas Government Code Chapter 791), authorizing the creation of the ARIC partnership, each Partner Agency's roles and responsibilities, and incorporating this Privacy Policy.

Law, as used in this policy, includes any applicable local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal officials or agencies.

Need to Know is established when, 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 counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Originating Agency is the Partner Agency that has contributed the information to the ARIC.

Partner Agency is a governmental agency that is listed in the ARIC Interlocal Agreement as a partner and has agreed to all ARIC privacy and operational policies enumerated therein.

Public includes:

(1) Any person and any for-profit or nonprofit entity, organization, or association;
(2) Any governmental entity for which there is no existing specific law authorizing access to ARIC's information;
(3) Media organizations; and
(4) 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 ARIC.

Public does not include:
(1) Employees of ARIC;
(2) People or entities, private or governmental, who have legal authority to assist the ARIC in the operation of the justice information system; and
(3) Public agencies whose authority to access information gathered and retained by the ARIC is specified in law.

Right to Know is established when, 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 a law enforcement, homeland security, or counter-terrorism activity.

Source agency is the agency that gathered data or information that is submitted to ARIC by the originating agency. The originating agency may also be the source agency.

Suspicious Activity is observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

Suspicious Activity Report (SAR) is the official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are SARs designed to support interagency calls for service.

III. POLICY APPLICABILITY AND LEGAL COMPLIANCE

A. All Partner Agency personnel, personnel providing information technology services to ARIC, private contractors, and any other authorized users will comply with the ARIC Privacy Policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to ARIC personnel Partner Agencies (including Information Sharing Environment [ISE] 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 ARIC shall make this policy available to the public through available resources, including the ARIC website and the City of Austin's website.

C. All personnel who provide services to ARIC and partner agencies and their individual users shall be provided with an electronic copy of this policy and will be required to provide a written acknowledgement of receipt of the policy and agreement to comply with its applicable terms and conditions. Such acknowledgements will be maintained by the Center.

D. All Partner Agencies and their personnel, personnel providing information technology services, private contractors, and other authorized users shall operate in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. and Texas Constitutions, state law, including, but not limited to the Texas Government Code Chapter 552 Public Information Act, and applicable Federal law, including 28 CFR Part 23.

E. ARIC has adopted internal operating policies that comply with the applicable law cited above and this policy.

IV. GOVERNANCE AND OVERSIGHT

A. Primary responsibility for the operation of the ARIC justice information and intelligence sharing system is assigned to the Austin Police Department (APD). The Center's governance shall consist of an Executive Board, Operational Management Team, Center Director, and Privacy Officer, each described below.

B. The Executive Board shall be comprised of the heads of the five major Law Enforcement entities in the Austin-Round Rock metropolitan area, or their designee(s), and chaired by the APD police chief or designee. The Executive Board shall meet as needed and agreed upon by Board members. This Board shall:

a. Resolve conflicts or disputes that might arise related to policy or mission;
b. Establish protocol concerning the treatment of violations of this Agreement;
c. Control the dissemination of any information produced by ARIC including specific alerts and bulletins to agencies inside and outside the region;
d. Resolve disputes between Partner Agencies arising from the operation and activity of the ARIC; and
e. Review and update the ARIC Privacy Policy annually based upon recommendations by the Privacy Policy Advisory Committee (described below), and changes in applicable law.
f. Shall provide an annual report to Partner Agencies on the status and efficacy of the Privacy Policy and ARIC based upon internal and external audits conducted and/or coordinated by the ARIC Operational Management Team (described below).

C. The APD police chief or designee will appoint a Center Director, who will be responsible for the day to day operation of the Center. The Center 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 Center Director shall coordinate with the Privacy Officer, described below, to ensure that enforcement procedures and sanctions as specified in subsection F., below, and Section VIII. A. are adequate and enforced.

D. The ARIC Operational Management Team (Management Team) will be responsible for: technology, use of ARIC information and intelligence databases, conducting and/or coordinating internal and external audits, and investigating misuse of the Center's data resources.

E. ARIC shall have a trained Privacy Officer who is appointed by the Center Director and who assists the Committee 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 prior to dissemination or sharing by the center. The Privacy Officer can be contacted through the ARIC website.

F. Privacy Policy Advisory Committee.

a. The Privacy Policy Advisory Committee (Committee) shall review the Privacy Policy annually to ensure safeguards, and sanctions are in place to protect personal information, and shall advise the Executive Board of ARIC of its recommendations based upon the purpose and mission statements of ARIC.

b. The Committee shall annually select from its membership a chair and any additional officers that the board finds appropriate. A person may not serve as the chair for more than two consecutive years. Upon selection of the chair and additional officers, the Committee shall agree upon the meeting schedule and other operational procedures.

c. The Committee shall include the following, as selected by the governing bodies or their designees:
   1. a community advocate, as selected by the City of Austin;
   2. a licensed attorney, as selected by Hays County;
   3. an information privacy advocate, as selected by the City of Round Rock;

4. a criminal justice expert, as selected by Travis County; and
5. a law enforcement expert, as selected by Williamson County.

d. The Committee shall provide a report to the Partner Agencies no less than once each calendar year that details all proposed or executed changes to the Privacy Policy. The report will include the results of any discussion, review and decision by the Executive Board regarding such changes

G. Individual users of the ARIC's information remain responsible for the lawful and appropriate use of the information and intelligence provided by ARIC. Failure to abide by the restrictions and use limitations for ARIC'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 individual user and Partner Agency participating in the ARIC is required to abide by this privacy policy in providing information and intelligence to the ARIC and in the access, use, security, and disclosure of information and intelligence obtained by and through the Center.

V. COLLECTION LIMITATION

A. All data will be obtained lawfully by contributing agencies, and for criminal intelligence information, in strict compliance with the Code of Federal Regulations, 28 CFR Part 23, and all other applicable federal, state, or local statute or ordinance and policy governing information gathering and information and intelligence collection practices.

B. The ARIC will not directly or indirectly knowingly receive, seek, accept, or retain information from an individual or nongovernment information provider, if the ARIC knows or has reason to believe that:

(1) The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the ARIC;
(2) The specific information sought from the individual or information provider could not be legally collected by the ARIC;
(3) The ARIC has not taken the steps necessary to be authorized to collect the information.

C. ARIC may only seek or retain information that was gathered in a fair and lawful manner, wherein the source is reliable and the content is valid or limitations on confidence are identified and with the knowledge and consent of the individual, if appropriate, and falls into the following categories:

(1) That relates to non-criminal threats to public health or infrastructure, and disaster response and relief; or

(2) Is suspicious activity that has a potential terrorism or criminal nexus and constitutes a SAR or ISE-SAR information under the Information Sharing Environment Functional Standard; or

(3) Is relevant to the investigation and prosecution of suspected criminal, including terrorist, activity, the justice system response, and the prevention of crime or is useful in crime analysis or in the administration of justice and public safety (including topical searches of open source information).

D. Within the Criminal Intelligence System, ARIC shall collect and retain information *only* where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorism) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity

E. This policy applies to information or intelligence that identifies any individual or organization as a criminal subject. The ARIC will not seek, collect or retain information about an individual or organization, and originating agencies will not submit such information, solely on the basis of religious, political, or social views or activities; participation in a particular organization or event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Further, these factors will not be considered as factors that create suspicion, except if used as part of a specific suspect description.

F. Information obtained from or through the ARIC can only be used for lawful purposes. A lawful purpose means the request for data is directly linked to a law enforcement agency's active criminal investigation, or is in response to confirmed information that requires intervention to prevent a criminal act or other threat to public safety. All information disseminated from the ARIC related to criminal activity that identifies a criminal subject must be relevant and useful in aiding an authorized and active criminal or background investigation.

G. Upon receipt of information collected by the center, ARIC personnel shall assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency 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
- the reliability of the source
- the validity of the content

H. At the time the decision is made by ARIC to retain information, it will be labeled 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 of privacy or their civil rights and liberties; and
- provide legally required protections based on the individual's status, such as a child, witness, sexual abuse victim

I. All labels assigned to existing information will be reevaluated at such times when new information is added that has an impact on access limitations or the sensitivity of disclosure of the information, or there is a change in the use of the information affecting access or disclosure limitations such as a change in case status.

J. The SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the Information Sharing Environment. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be gathered documented, processed, and shared either intentionally or inadvertently.

K. All SAR information submitted by source agencies will be gathered and reviewed by law enforcement officers and supervisors trained to recognize terrorism behaviors and SAR information collected will be processed and undergo a two-step assessment by trained ARIC analysts or investigators as set forth in the ISE-FS-200, to determine that it was legally gathered and meets the criteria for placement in the ARIC ISE shared space. ARIC will secure SAR and ISE-SAR information in a separate repository system that meets 28 CFR Part 23 security requirements and adheres to the Functional Standard and established policies for ISE-SAR information under the Nationwide Suspicious Activity Reporting Initiative (NSI) in the collection, use, storage, and sharing of SAR and ISE-SAR information. This includes the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-FS-200 for suspicious activity potentially related to terrorism. SAR and ISE-SAR information will not be merged into other reports, files, and documents. In addition, ARIC personnel will adhere to the following practices and procedures for the collection, assessment, retention/storage, security, and sharing of SAR and ISE-SAR information:

(1) Prior to sharing the information, ensure that attempts to validate or refute the information have taken place, the information has been assessed and labeled for sensitivity and confidence, and the ARIC reporting format and data collection codes for SAR information have been used.

(2) Provide access or disseminate the information to partner agencies in response to authorized inquiries and analytical purposes or provide an assessment of the information (without personal identifiers) to any agency, organization, or individual,

including the public, when credible information indicates potential imminent danger to life or property.

(3) Retain ISE-SAR information that is unconfirmed for up to two years in order to validate a tip, lead, or other SAR information to determine its credibility and value, and, if confirmed, for up to a total of five years unless it is validated prior to its expiration for an additional retention period. Information shall be assigned a disposition label 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 and consistent with total retention periods.

L. The ARIC incorporates the collection, assessment, retention/storage, security, and sharing of SAR and ISE-SAR information into existing processes and systems used to manage other crime related information to protect information and intelligence, as well as privacy and civil liberties. All constitutional protections and individual agency policies and procedures that apply to a law enforcement officer's authority, for example, to stop, detain, identify, search and frisk, will be followed and upheld in the same measure when gathering SAR information, whether or not the observed behavior is related to criminal activity.

M. The ARIC will identify and review protected information that is held by the center prior to sharing that information through the Information Sharing Environment in order to ensure that to ensure that it provides the notice mechanisms required under Section IV., E. and F, above.

N. The ARIC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information include:

- The name of the originating department, component, and subcomponent.
- The name of the agency'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.

O. The ARIC will attach (or ensure that the originating agency 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.

P. The ARIC will keep a record of the source of all information retained by the center.

VI. INFORMATION SHARING

A. Access to information and intelligence contained within the ARIC's databases will be granted only to ARIC and authorized Partner Agency user personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Operational Management Team and individual Partner Agencies. Each individual user obtaining information will be required to acknowledge, in writing, that he or she remains solely responsible for the interpretation, further dissemination, and use of the information 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 (see E., below). Further, access is limited to legitimate law enforcement, public protection, prosecution, public health or justice purposes and only in the performance of official duties in accordance with the law and policies applicable to the agency for which the person is working.

B. The decision of each Partner Agency to participate in the ARIC and the decision of which databases to make available is voluntary and will be governed by the laws and rules governing the individual agencies in respect to such data, as well as by applicable law. Information gathered and investigation techniques used by Partner Agencies will comply with all applicable law.

C. The ARIC will not knowingly receive, seek, accept, or retain information from an individual or non-government information provider, including commercial data providers, if ARIC knows or has reason to believe that the individual or information provider obtained specific information that could not be legally obtained by the ARIC. The ARIC will ensure it has taken the steps necessary to be authorized to collect the information. In addition, commercial data providers shall provide an assurance that the data was lawfully gathered using methods not based on misleading information collection practices. The ARIC will only pay a fee or benefit for information provided by authorized commercial database entities authorized under applicable ARIC policy and will not directly or indirectly seek, receive, accept, or retain information from a provider that is legally prohibited from obtaining or disclosing the information.

D. The ARIC will not allow original materials gathered or collected under these policies to be removed from the Center unless necessary to be used as evidence in a criminal matter, with the exception of removal in accordance with applicable laws, records retention policies, or court order.

E. In order to maintain the integrity of the ARIC, any information obtained through the Center must be independently verified with the source from which the data originated prior to any official action being taken by the ARIC or a Partner Agency.

VII. RECORD RETENTION

A. The ARIC will comply with all applicable federal, state, and local laws, rules, and regulations, and applicable originating agency policies regarding the retention of records held by the Center.

B. All information held by the ARIC will be subject to review by the Executive Board. Information that is misleading, irrelevant to ongoing criminal investigations, obsolete, or otherwise unreliable will be immediately purged, without the approval of the originating agency, from the ARIC information system. The ARIC will notify originating agencies of all alleged errors (See Data Quality), changes made, and data purged. The ARIC will maintain a record of information to be reviewed for retention. Originating agencies will not be notified of pending expiration dates for information held by the ARIC, which will purge such information, without the approval of the originating agency, if it is not validated by the originating agency prior to its expiration date. Criminal intelligence information retained after the Committee's ongoing review or originating agency review must reflect the name of the reviewer, date of review, and reason for retention, in accordance with 28 CFR Part 23. Ongoing review of all information will continue until the expiration of the retention period.

C. The retention period of all information held by the ARIC will be no longer than five years, unless validated for additional retention.

VIII. DISSEMINATION OF INFORMATION

A. Information will be provided to Partner Agencies in accordance with applicable law, the Interlocal Agreement between the Partner Agencies, and this Policy. The ARIC will use credentialed, role-based access criteria, as appropriate, to control information access, authority to add, change, delete, or print, and to whom the information can be disclosed and under what circumstances. All Partner Agency personnel who receive, handle, or have access to the ARIC databases will be thoroughly trained as to this policy. Unauthorized access or use of the ARIC's resources is prohibited. The ARIC reserves the right to restrict Partner Agency personnel from access to the center and to suspend or withhold the access rights of any individual or agency violating this Privacy Policy. The Executive Board shall be notified of any individual's or agency's restriction or suspension of access to ARIC by the Center Director. Any use of the ARIC's data in an unauthorized or illegal manner will subject the individual user to denial of further use or access to the ARIC, discipline by the user's employing agency, and/or criminal prosecution.

B. Information obtained from or through the ARIC will not be used or publicly disclosed for purposes other than as specified in this Privacy Policy and the Interlocal Agreement that each Partner 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; (3) disseminated to unauthorized persons; or (4) used in any way that is otherwise inconsistent with the statutes, rules, policies or procedures that govern the ARIC and its Partner Agencies.

C. Information that would interfere with or compromise pending criminal investigations shall not be disseminated publicly unless required by law or as determined by the Executive Board of the ARIC and with the agreement of the contributing agency.

D. A Partner Agency will not disclose information originating from another agency except as authorized by such agency and/or required by law.

E. Members of the general public cannot access individually identifiable information on themselves or others from the ARIC unless such disclosure is required by law. 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. Such requests shall be documented by that agency, including what information, if any, was disclosed to a member of the public. The ARIC Privacy Officer shall be the individual responsible for receiving and responding to such inquiries and/or complaints regarding information held by ARIC.

F. If, upon receipt of requested information, an individual believes such information is inaccurate, incomplete, or otherwise deficient, that individual may contact the Center and request correction. An individual to whom information has been disclosed will be given reasons if requests for correction are denied by ARIC or the originating agency, including ISE participating agencies. The individual will be informed of the procedure for correction of the challenged information and appeal if a request for correction is denied, in whole or in part, and/or directed to the originating agency for further review and appeal. A record will be kept of all requests for corrections and the resulting action, if any.

G. If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the ARIC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the ARIC will inform the individual of the procedure for submitting and resolving complaints or objections. Complaints will be received by the Privacy Officer through the Austin Police Department at P.O. Box 689001, Austin, Texas, 78768, or electronically through the ARIC website (a link to this website is provided through the Austin Police Department site). The ARIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure. If the information did not originate with the ARIC, ARIC will notify the originating agency in writing within 10 days and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify that the record is accurate. Any personal information originating with the ARIC or an originating agency will be reviewed and corrected in or deleted from ARIC data/records within 30 days of the complaint or notice to an originating agency if it is determined to be erroneous, include incorrectly merged information, or out of date. If the ARIC has not confirmed or denied the error or deficiency within 30 days, the ARIC will not share the information until such time as the complaint has been resolved. A record will be kept of all complaints and the resulting action, if any.

H. The ARIC shall maintain records of agencies sharing terrorism-related information and audit logs and employ system mechanisms to identify the originating agency when the information is shared in order to delineate protected information shared through the ISE from other law enforcement data.

IX. DATA QUALITY

A. ARIC Partner Agencies remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data provided to the Center. The ARIC will make every reasonable effort to seek and retain only information that is derived from credible sources and that is accurate, current, and complete. Such information, other than SAR and ISE-SAR information, will be merged with existing information on an individual or organization only when sufficient identifying information (for example, fingerprints, photograph, and/or contact information) is available to reasonably conclude the information is about the same individual or organization. ISE-SAR information will not be disseminated to partner agencies unless there is a need and right to know the information in the performance of a law enforcement, homeland security, or public safety activity. An audit trail will be kept of access by or dissemination of information to all recipients. In accordance with this policy, all information will, when retained, be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

B. The ARIC shall investigate, in a timely manner, alleged errors and deficiencies in data and records (or refer them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

C. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (i.e., validity and reliability) in previously retained information.

D. The ARIC will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the center; or the source used prohibited means to gather the information (except when the source did not act as an agent to a bona fide law enforcement officer).

E. The ARIC will advise the appropriate contact person in the originating agency, in writing, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

F. The ARIC will use written or documented electronic notification to inform all recipient agencies when information previously provided to the recipient agency is deleted or changed by the ARIC; for example, when 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.

X. COLLATION AND ANALYSIS

A. Information acquired or received by the ARIC 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 according to policy established by the Operational Management Team and Executive Board.

B. Information subject to collation and analysis is information as defined and identified in Section IV., Collection.

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

(1) Further crime prevention, including terrorism, enforcement, force deployment, or prosecution objectives and priorities established by the ARIC, and
(2) Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities.

XI. SECURITY SAFEGUARDS

A. The Center Director shall designate a trained, ARIC-assigned employee to serve as the ARIC's security officer. The security officer, in coordination with the Privacy Officer, shall document and report internal and external breaches of security and violations of policy regarding technology within the Center to the Operational Management Team.

B. The ARIC will operate in a secure facility protecting the facility from external intrusion, utilizing secure internal and external safeguards against network intrusions. Access to ARIC databases from outside the facility will be allowed only over secure networks.

C. The ARIC will secure SAR and ISE-SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion.

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

E. Access to ARIC information will be granted only to ARIC-assigned 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 ARIC data applications will be logged into the data system identifying the user initiating the query.

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

H. When information has been breached or obtained by an unauthorized person, and the release of such information may threaten physical, reputational, or financial harm to an individual or agency, the ARIC shall promptly notify the individual and the source agency. The ARIC 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 information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

XII. COMPLIANCE, ACCOUNTABILITY, AND ENFORCEMENT

A. It is the intent of the ARIC to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. All Partner Agencies will make this Privacy Policy available to the public upon request.

B. Partner Agencies will adopt and comply with internal policies and procedures requiring the agency, its personnel, contractors, and users to:

(1) Have and enforce policies for discovering and reporting violations of the ARIC Privacy Policy, including taking appropriate action when violations are found;

(2) Provide training, as agreed to by the Executive Board, to personnel authorized to use the ARIC justice information sharing network regarding the ARIC's requirements and policies for information gathering, submission, collection, use, storage, and disclosure;

(3) Make available to the public the agency's internal policies and procedures regarding privacy, civil rights, and civil liberties protection as required by the Texas Public Information Act;

(4) Cooperate with periodic, random audits by representatives of the ARIC justice information sharing system; and

(5) Designate an individual within the Partner Agency to receive reports of alleged errors in information that originated from the Partner Agency.

C. The ARIC Operational Management Team will adopt procedures and practices, approved by the Executive Board, by which it can ensure a proper evaluation of the compliance of users with user responsibilities under the provisions of this policy and applicable law. This will include logging access of these systems and annual and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated and a record of the audits will be maintained by the Privacy Officer of the agency.

D. The ARIC's personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information to the ARIC Privacy Officer. The Privacy Officer shall report violations to the Center Director in a timely manner. The ARIC Privacy Officer will also be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information systems maintained or accessed by the ARIC. The Privacy Officer can be contacted through the ARIC Web site.

E. The ARIC will annually conduct an audit and inspection of the information contained in its criminal intelligence system. The audit will be conducted by the ARIC Operational Management Team or a designated independent panel. The audit authority has the option of conducting a random audit, without announcement, at any time and without prior notice to the ARIC. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the ARIC's criminal intelligence system.

F. The ARIC Executive Board will prepare an annual report to the City Council regarding Privacy Policy and data access issues as well as audit results.

G. ISE-SAR information will not be disseminated to partner agencies unless there is a need and right to know the information in the performance of a law enforcement, homeland security, or public safety activity. An audit log of queries and an audit trail will be kept for a minimum of two years of access by or dissemination of information to all recipients.

XIII. TRAINING

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

- All assigned personnel to ARIC,
- Personnel directly providing information technology services to the ARIC,
- Staff in other public agencies or private contractors providing services directly to ARIC,
- Users who are not employed by ARIC or a contractor.

B. The ARIC will provide special training to personnel authorized to share protected information through the ISE regarding the ARIC's requirements and policies for collection, use, and sharing of such information.

C. The ARIC's 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 the ARIC;
- 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 the agency;
- Mechanisms for reporting violations of agency/center privacy-protection policies; and
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.