Privacy Policy
Version 3.4

Covers the operations of the Florida Fusion Center, participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to the FFC.

Table of Contents

A. Intent

The intent of this policy is to ensure that the Florida Fusion Center (FFC) protects both the security of the people of the State of Florida as well as their privacy interests. The FFC is committed to the responsible and legal compilation and utilization of criminal investigative information, criminal intelligence information, and other information important to protecting the safety and security of the people, facilities, and resources of the State of Florida and the United States. All compilation, utilization, and dissemination of information by FFC participants and source agencies will conform to requirements of applicable state and federal laws, regulations and rules. The FFC will also abide by privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines, State and Major Urban Area Fusion Center Baseline Capabilities, the National Suspicious Activity Reporting (SAR) Initiative, 28 CFR Part 23, and, to the greatest extent possible, the Fair Information Practice Principles.

All local, state, tribal and federal agencies participating with the FFC by virtue of submitting, receiving or disseminating criminal intelligence or criminal investigative information, SAR information, tips or leads via the FFC are required to adhere to the requirements of the FFC Privacy Policy when participating in the activities of the FFC.

B. Background

Fusion centers are a collaborative effort of two or more agencies that provide resources, expertise, and/or information with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity utilizing an all crimes/all hazards approach. Fusion centers are an outgrowth of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) which directed the establishment of an Information Sharing Environment (ISE) across all levels of government. Fusion centers help to fulfill the mission of information sharing efforts across the spectrum of federal, state, tribal, territorial, and local entities by collecting and analyzing information, which could be vital to supporting law enforcement, domestic security, and public safety missions.

The FFC is located within the Florida Department of Law Enforcement's (FDLE) Office of Statewide Intelligence, located in Tallahassee, Florida, and consists of federal agencies, state multi-disciplinary partners, regional fusion nodes, local law enforcement and criminal justice agencies. Information used by the FFC includes criminal intelligence information, criminal investigative information, tips, leads, and SARs documented by local, state, tribal and federal agencies in a variety of systems to include the designated Florida statewide intelligence system.

C. Purpose

The purpose of this privacy policy is to ensure the FFC and its members comply with applicable federal, state, local and tribal laws, regulations, and policies and assist all parties in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Increasing public safety and domestic security while maintaining appropriate levels of transparency.
- Protecting the integrity of systems used for the observation and reporting of criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.

D. Definitions

Criminal Intelligence Information — Information with respect to an identifiable person or group of persons collected by a criminal justice agency in an effort to anticipate, prevent, or monitor possible criminal activity. Per 28 C.F.R. Part 23, criminal intelligence information meets the threshold for retention when the information is relevant to an individual or organization who is reasonably suspected of involvement in criminal acts.

Fair Information Practice Principles — The Fair Information Practices Principles (FIPPs) are contained within the Organization for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transporter 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 justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. To the extent practicable, an integrated justice system should be designed to meet the following principles:

1. *Purpose Specification Principle* - Define agency purposes for information to help ensure agency uses of information are appropriate.
2. *Collection Limitation Principle* - Limit the collection of personal information to that required for the purposes intended.
3. *Data Quality Principle* - Ensure data accuracy.
4. *Use Limitation Principle* - Ensure appropriate limits on agency use of personal information.
5. *Security Safeguards Principle* - Maintain effective security over personal information.
6. *Openness Principle* - Promote a general policy of openness about agency practices and policies regarding personal information.
7. *Individual Participation Principle* - Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency.

Personally Identifiable Information — Personally identifiable information is 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, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number). Descriptions of 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.).

Privacy — Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable 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.

Suspicious Activity and Suspicious Activity Reports — Observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. Suspicious Activity Reports (SARs) are official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.

Tips and Leads — Tips and leads are defined as reported or observed activity and/or behavior that, based on an officer or analyst's training and experience, is reasonably believed to be indicative of intelligence gathering or preoperational planning related to non-terrorism criminal activity. Tips and leads are distinguished from SARs due to their lack of nexus to terrorism, but are treated similarly in all other regards in this policy.

E. Policy Applicability and Legal Compliance

All FFC members, participating agency members, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with this Privacy Policy, as well as any applicable laws and policies protecting privacy, civil rights, and civil liberties.

All FFC members are operating under a Memorandum of Understanding and each member is required to sign an Information Security Agreement to participate. Information Security Agreements are written with the intent to protect sensitive information while comporting with transparency and accountability expectations codified in Florida's sunshine laws. These agreements are physically maintained in the FFC and the FDLE Office of General Counsel. All agencies providing criminal intelligence, tips, leads, or SAR information to the designated Florida statewide intelligence system are operating under Agency User Agreements and Individual User Agreements, which are physically maintained by the FDLE.

Any FFC activity pertaining to the identification and submission of information, access to, or disclosure of information will comport with this Privacy Policy. All participants and members of the FFC are required to review, acknowledge and adhere to the FFC Privacy Policy. All participants and source agencies, to include all individual users of the designated Florida statewide intelligence system, are required to review and adhere to the FFC Privacy Policy. The FFC will provide a printed copy of this policy upon request to all entities participating in the FFC and will require a written acknowledgement to comply with this policy and the provisions it contains. The FFC Privacy Policy is posted on the FFC public website. The FFC Privacy Policy will also be posted on FFC-controlled intelligence systems.

The FFC has adopted internal operating policies and/or procedures, all of which will be compliant with this Policy, as well as applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, the U.S. Constitution and the Florida Constitution as well as applicable state, local, and federal laws and regulations regarding privacy, civil rights, and civil liberties. The FFC will comply with all applicable public record laws pertaining to criminal intelligence and criminal investigative information.

F. Membership of the FFC

All government agencies participating in operations of the FFC must enter into a memorandum of understanding (MOU) with the FDLE outlining and agreeing to the terms and agreements for such participation. Participating governmental agencies will assign an Executive Board member and an Intelligence Liaison to the FFC. Members assigned to the FFC will be expected to participate in a capacity as deemed appropriate by the member's agency and will have the ability to be virtually connected to the FFC. FFC membership is restricted to designated Executive Advisory Board members, Intelligence Liaison Officers (ILOs) and Interagency Fusion Liaisons (IFLs) from local, state, tribal, federal agencies, trusted private partners and FDLE personnel. Regional fusion centers and their employees that have been adopted as certified nodes of the FFC shall also be considered FFC members.

All FFC members must adhere to training requirements set forth by the FDLE for the FFC. These training requirements include training on 28 CFR Part 23, which will be on an annual basis, as well as annual refresher training on the FFC Privacy Policy and Standard Operating Procedures.

G. Governance and Oversight

Primary responsibility for the operation of the FFC is assigned to the FDLE Special Agent in Charge of OSI and the FFC Director, who is appointed internally by the FDLE. The Director of the FFC will have the responsibility for ensuring compliance by members from the FFC, as well as embedded assets from partner agencies. All FFC members are personally responsible, and will be personally accountable for, adhering to this Policy, maintaining information standards, processes, procedures and practices. Individuals assigned to the FFC from agencies outside FDLE are also bound by an Information Security Agreement, to the extent allowable by law.

The FFC is also guided by the FDLE Office of the General Counsel and its designated Privacy Officer to assist in the enforcement of the provisions of this policy. The Privacy Officer will receive and review reports regarding alleged errors and violations of this policy and provide recommendations to the FFC Director to ensure compliance.

The FFC requires that all FFC analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties (P/CRCL) protections prior to dissemination or sharing by the center. The FFC maintains the same P/CRCL standards for pass-through information provided by other entities, and the Privacy Officer will maintain visibility on all information provided through the FFC.

H. Acquiring and Receiving Information

1. Information gathering and investigative techniques used by the FFC, affiliated agencies and all personnel assigned to the FFC will comply and adhere to the following regulations and guidelines:
   - The FFC will follow 28 CFR Part 23 with regard to the collection and retention of criminal intelligence information.
   - The FFC will adhere to criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
   - The FFC will adhere to all obligations of law, including Florida's public records laws, as well as any regulations that apply to multi-jurisdictional intelligence databases.

2. Regardless of the criminal activity involved, no information which a user has reason to believe may have been obtained in violation of law shall be used or retained by the FFC unless and until its legality can be verified. If the FFC is notified or otherwise learns that information has been obtained illegally, it will be immediately purged from FFC intelligence systems, absent a need to retain the information for an accountability review.

3. Agencies that participate in the FFC and which provide information to the FFC are governed by state and local laws and rules governing them, as well as by applicable federal laws. The FFC will not knowingly contract with commercial database entities that demonstrate that they gather personally identifiable information out of compliance with local, state, tribal, territorial, and federal laws, or which is based on misleading information collection practices.

4. The FFC will not directly or indirectly receive, seek, accept, or retain information from any individual or provider if the FFC knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information, or if the FFC has reason to believe that the source used prohibited means to gather the information.

5. The FFC will only seek or retain information that:
   - Constitutes a credible criminal predicate or a potential threat to public safety based on at least a reasonable suspicion standard; or
   - Demonstrates by at least a reasonable suspicion threshold that an identifiable individual or organization has committed, is committing, or is planning to commit criminal conduct or activity that presents a threat to any individual, community, or the nation; or
   - Is relevant to an active or ongoing investigation and prosecution of a suspected criminal incident; the resulting justice system response, the enforcement of sanctions, orders, or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort; and
   - Is such that the source of the information is reasonably believed to be reliable and is verifiable and, when appropriate, the limitations on the reliability or veracity of the information is clearly stated; and
   - Is information that was collected in a fair and lawful manner.

6. The FFC will not seek or retain 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 race, ethnicity, nationality, place of origin, age, disability, gender, gender identity or sexual orientation. Information related to these factors may be retained if there is a relevance between such information and the effort to detect, anticipate, or prevent criminal activity, there is at least a reasonable suspicion that criminal activity may be upcoming or ongoing, and this information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal nexus exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or FFC members to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information.

7. The FFC and its members are prohibited from collecting information on public events for investigative purposes, to include protests, demonstrations and rallies, unless there is a reasonable articulable suspicion of potential criminal activity or public safety threats associated with an event. The FFC will not collect the personally identifiable information (PII) of any event attendees unless there is reasonable suspicion that the attendee(s) is involved

in criminal activity. Any information shared by the FFC and its partners on public events will not use such information for criminal intelligence or investigative purposes, but instead such information may be provided only for situational awareness due to the potential for large crowds, disruption of public proceedings and traffic flow, and the potential for criminal elements or extremists to exploit protected activities by utilizing these platforms to conduct violent or criminal acts.

I. SARs, Tips and Leads

The FFC is a participant in the Information Sharing Environment (ISE) National SAR Initiative (NSI). SARs with a nexus to terrorism will be provided to the designated national suspicious activity reporting system by the FFC after appropriate review. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center, the appropriate FDLE Regional Operations Center and Joint Terrorism Task Forces. SARs are 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. Other forms of terrorism information shared in the ISE by the FFC will be in accordance with the ISE Privacy Guidelines.

1. The FFC's SAR, tips and leads process provides for human review and vetting to ensure that information is both gathered in an authorized and lawful manner and, when applicable, determined to have a potential terrorism nexus. FFC members who acquire SAR information that may be shared with the FFC will be trained to recognize behavior that is indicative of criminal activity related to terrorism. The FFC will ensure all members receive biennial SAR refresher training.

2. Access to and use of ISE-SAR information will comply with all relevant laws and regulations including those derived from the U.S. Constitution, the Florida Constitution, applicable federal and state laws and local ordinances, and the Office of the Program Manager for the Information Sharing Environment (PM-ISE) policy guidance applicable to the ISE-SAR initiative.

3. FFC participating agency members in receipt of designated SAR information will:
   - Review and vet the SAR information and provide the two-step assessment set forth in the NSI functional standard as outlined in the FFC Standard Operating Procedures to determine whether the information qualifies as an ISE-SAR for contribution to the designated national suspicious activity reporting system.
   - Provide appropriate reliability and validity labels.
   - Ensure that SAR information is not based on immutable characteristics of individuals or Constitutionally protected activities. FFC members are not permitted to engage in intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality.

4. When a choice of investigative techniques is available, information documented as a SAR, tip, or lead should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation. The FDLE adheres to investigative and operational practices that meet all Commission on Accreditation for Law Enforcement Agencies (CALEA) standards and which are memorialized in an FDLE Procedures Manual. These practices reflect the need to balance privacy, civil rights, and civil liberties with law enforcement investigative operations.

5. At the time a decision is made to contribute SAR information to the designated national suspicious activity reporting system, FFC members or source agency personnel will label it (by record, data set, or system of records and to the extent feasible, consistent with NSI functional standards) pursuant to applicable limitations on access and sensitivity of disclosure.

The FFC will retain tips, leads, or SARs within the designated Florida statewide intelligence system only for the length of time necessary to determine if it has criminal intelligence value. As a general rule, SARs, tips, and leads should be reviewed and evaluated for contemporaneous value within 90 days and, if deemed noncredible, will be purged as soon as permissible pursuant to applicable Florida Department of State retention schedules. In addition, FDLE may require a contributing agency to justify why any particular tip, lead, or SAR should remain in the system if it appears to FDLE that the information is no longer active or otherwise of intelligence or investigative value. Failure to satisfy FDLE's request may result in the information being unilaterally removed from the system by FDLE. Notice of any such removal will be made to the contributor.

1. Intelligence information, SARs, tips and leads will be removed or requested to be removed from the applicable reporting system or database if it is determined the source agency did not have the authority to acquire the original information, used prohibited means to acquire it, or did not have the authority to provide it to the FFC or the relevant system. Information subject to an expungement order in state or federal court that is enforceable under state law or policy will also be removed from the designated Florida statewide intelligence system and the designated national suspicious activity reporting system.

2. The FFC's SAR, tips and leads 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 will be documented and shared. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed, and shared.

3. If FFC personnel believe that a SAR, tip or lead containing PII may meet the basic threshold for sufficiency but is based on behaviors that are not inherently criminal (e.g. photography of secure areas at a critical infrastructure facility), the FFC will seek additional fact development during the vetting process. The FFC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

J. Vetting and Storage of Information

1. The FFC requires certain basic descriptive information to be entered and electronically associated with data (or content), SARs, tips and leads, and intelligence products that are to be accessed, used, and disclosed, including:
   - The name of the originating department or source agency.
   - The date the information was collected and to the extent possible, the date its accuracy was last verified.
   - To the extent possible, data fields will indicate whether the record includes protected information, to include information about U.S. persons, lawful permanent residents or PII.

- The title and contact information for the person to whom questions regarding the information should be directed, as well as the individual accountable for the decision to submit the information and the assurance of its conformity to FFC submission standards.
- Any particular limitations to the use or disclosure of the information based on the classification or sensitivity of the information or other similar restrictions on access, use or disclosure, and if so the nature of those restrictions.
- To the extent possible, the source reliability and the information validity will be assessed and documented.

2. The FFC participating agency members will, upon receipt of information, to include SARs, tips and leads, assess the information to determine its nature and purpose. Members of the FFC will assign information to categories to indicate the result of the assessment, such as:
   - Whether the information is a tip, lead, SAR, or criminal intelligence information;
   - The nature of the source (for example, criminal justice or public safety agency, anonymous tip, interview, open source/public records, private sector);
   - The relevance of PII, ideological associations, and/or personal descriptive information to the underlying criminal or suspicious behaviors. The FFC will only document such traits if they have a direct relevance to potential criminal activity;
   - The reliability of the source:
     - Reliable – The reliability of the source is unquestioned or has been tested in the past and proved dependable.
     - Usually reliable - The reliability of the source can usually be relied upon as factual. The majority of the information in the past has proven to be reliable.
     - Unreliable – The reliability of the source has been sporadic in the past.
     - Unknown – The reliability of the source cannot be judged. Its authenticity or trustworthiness has not been determined by either experience or investigation.
   - The validity of the content:
     - Confirmed – The information has been corroborated by an investigator or analyst or another independent, reliable source.
     - Probable - The information is logical and consistent with other relevant information but has not been confirmed.
     - Doubtful – The information has not been confirmed and is not logical and/or consistent with other relevant information.
     - Cannot be judged – The information cannot be judged at the current time. Its authenticity had not yet been determined by either experience or investigation.
   - Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be “unknown” and content validity “cannot be judged.” In such case, users must independently confirm source reliability and content validity with the source, submitting agency or through their own investigation.
   - Due diligence will be exercised by all participating agencies in determining source reliability and content validity. FFC members may reject information as failing to meet any criteria for inclusion.
   - Information determined to be unfounded will be purged from any FFC controlled systems.

3. FFC members are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tip, lead and SAR information.
   - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information. The

storage of SARs, tips and leads will be through the designated Florida statewide intelligence system.

- Allow access to, or disseminate, the information using the same (or a more restrictive) access or dissemination method 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).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of criminal intelligence information when credible information indicates potential imminent danger to life or property.
- Retain information long enough to work a tip or lead to determine its credibility and value, assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows that status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.
- Adhere to and follow the FFC’s physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SARs will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.
- Routinely and regularly review information to determine if it should be purged.

4. The FFC will maintain a record of all formal requests for information (RFIs) to which it responds from other criminal justice or public safety agencies that are participating FFC members, other fusion centers, and criminal justice agencies

K. Collation and Analysis

1. Information acquired by the FFC or accessed from other sources, to include ISE-SAR information, will only be analyzed by qualified individuals who have successfully completed a background check, been selected, approved, and trained accordingly, and if applicable, obtained an appropriate security clearance. Individuals from participating FFC agencies must sign and adhere to this Privacy Policy and an Information Security Agreement.

2. Information acquired by the FFC or accessed from other sources is analyzed according to priorities and needs and will only be analyzed to:
   - Further crime/terrorism prevention, enforcement, force deployment, prosecution objectives or priorities established by the FFC, and
   - 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, including criminal solicitations, criminal conspiracies, and/or attempts to obstruct justice.

L. Information Quality Assurance

1. To the extent possible, the FFC will implement the “Fair Information Practice Principles” as detailed by the Department of Justice’s Global Initiative, recognizing that some of the practices (such as allowing individuals about whom information is retained to review the information for accuracy) may apply, at best, in a restricted fashion to an intelligence-gathering enterprise. All contributors of information to the FFC should be familiar with the Global “Fair Information Practice Principles” and apply those practices to the best extent

practicable to the information gathered, retained, reported to, and disseminated from the FFC.

2. The FFC will make every reasonable effort to ensure that information sought, retained, or disseminated, to include ISE-SAR information, tips and leads, and intelligence products, is derived from dependable and trustworthy sources of information; 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 has been met.

3. State, Local, Tribal, and Territorial (SLTT) agencies, including agencies participating in the FFC, are primarily responsible for the quality and accuracy of the data accessed by, or shared with the FFC, to include SAR data. At the time of sharing, intelligence information will be labeled according to the level of confidence in the information to the maximum extent feasible. The labeling of intelligence information will be periodically evaluated and updated when new information is acquired that has an impact on confidence in the information.

4. Information provided through the designated Florida statewide intelligence system by the FFC is not designed to provide users with information upon which official actions may be taken. The mere existence of records in the Florida statewide intelligence system or provided by the FFC should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant, or serve as documentation in court proceedings. The source agency should be contacted to obtain and verify the facts needed for any official action.

5. When the FFC receives or acquires new information relevant to an existing FDLE or FFC intelligence product, SAR, tip or lead, FFC members will evaluate whether said information has a bearing on the record's current labeling. This review will include an evaluation of the following data/record factors:
    - Accuracy
    - Currency
    - Reliability
    - Validity

    If this review indicates that there is a reasonable belief that the rights of an individual may have been violated, the FFC will notify the original agency and may, as appropriate, notify the affected individual.

6. The FFC will notify participating agencies when a review of FFC products indicates that information provided by the FFC may be inaccurate, incomplete, incorrectly merged, or cannot be verified. Any needed corrections or deletions will be made in the appropriate system.

M. Merging Records

1. Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude 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 higher accuracy of match.

2. Sufficient identifying information may include the name (full or partial) and in most cases, one or more of the following:
   - date of birth;
   - law enforcement or corrections system identification number;
   - individual identifiers, such as fingerprints, facial features/nodal points, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars;
   - social security number; or
   - driver's license number.

   The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same subject organization may include the name, federal or state tax ID number, office address, and telephone number. The reality that identities can be stolen by those who perpetrate crimes makes the verification of factors in support of merging of records particularly important. Innocent individuals' identities may be utilized by criminals and merging of an innocent individual's information into records related to the criminal without explanation or other appropriate safeguards against misinterpretation of the information should not occur.

3. If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization and a reminder that identity theft may be the reason there has been the partial match.

N. Sharing and Disclosure

1. Credentialed security access will be utilized to control:
   - To what information a class of users can have access;
   - To what information a class of users can add, change, delete, or print; and
   - To whom the information can be disclosed and under what circumstances.

2. Personally identifiable information (PII) will be removed from disseminated products as appropriate, particularly when not necessary or relevant to the product's purpose.

3. Agencies contributing information to the FFC will indicate at the time of submission the intent to have said information disseminated by FFC to other appropriate fusion or criminal justice, or public safety partners. In the absence of a request for additional dissemination, the FFC will operate according to the Third Agency Rule unless otherwise instructed by law, rule or Memorandum of Understanding; therefore, FFC participating agencies may not unilaterally disseminate information received from FFC without approval from the originator of the information. There is a presumption that all records contributed to the designated Florida statewide intelligence system and the designated national suspicious activity reporting system are intended to be shared with other agencies participating in said systems.

4. Florida has broad public record laws that may require disclosure in contravention to an originating agency's wishes. However, the FFC considers it a best practice to reach out to the originating agency prior to releasing information as part of a public records request.

5. Records retained by the FFC may be accessed or disseminated to those responsible for law enforcement, public health and safety protection, prosecutions, or criminal justice purposes

derived from criminal investigations or prosecutions only for such purposes and then only in the performance of official duties in accordance with applicable laws, regulations, and procedures. Records will be kept of access or dissemination of information to such persons in the event an audit is required. Information gathered and records retained by the FFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users or purposes specified by law.

6. FFC members or source agency personnel will label criminal intelligence information pursuant to applicable limitations on access and sensitivity of disclosure in order to:
   - Protect an individual's right to privacy and their respective civil rights and civil liberties;
   - Protect confidential sources and police undercover techniques and methods;
   - Not interfere with or compromise pending criminal investigations; and
   - Provide any legally required protection based on the individual's status as a child, sexual abuse victim, crime victim, resident of a substance abuse treatment program, resident of a mental health treatment program, resident of a domestic abuse shelter, or any other applicable protection.

7. Information and records retained by the FFC, to include intelligence or investigative information, ISE-SAR information, tips and leads, and those records within the designated Florida statewide intelligence system, that constitute active criminal investigative or active criminal intelligence information, or is otherwise within the scope of an applicable exemption or confidentiality provision of Florida law, will not be released to the public. Such information shared by the FFC may be disclosed to a member of the public only if the information is defined by law to be public record, or otherwise appropriate for release to further the FFC mission, and is not exempt or prohibited from disclosure by law.

8. The FFC shall not confirm the existence or nonexistence of information, to include designated Florida statewide intelligence system records or ISE-SAR information to any person or agency that would not be eligible to receive the information itself. ISE-SAR information will not be provided to the public if, pursuant to applicable law, it is:
   - Required to be kept confidential or exempt from disclosure.
   - Classified as active criminal investigative or intelligence information and exempt from disclosure.
   - Protected federal, state, or tribal records originated and controlled by the source agency that cannot be shared without permission.

9. Information that is no longer active criminal investigative or active criminal intelligence information will be promptly purged from FFC controlled systems in a manner consistent with Florida law.

10. Information gathered and records retained by the FFC will not be sold, published, exchanged, or disclosed for commercial purposes. It will not be disclosed or published without prior notice to the contributing agency. Information will not be disseminated to unauthorized persons.

O. Redress

1. As an entity housed with the FDLE, the FFC processes records requests through networks and systems controlled by FDLE. The FFC does not maintain records for all fusion centers across the state, and can only process requests through FDLE components. If an individual

wants to review information or intelligence documented by the FFC, a formal public records request must be made via the Florida Department of Law Enforcement. Records of public records requests made to FDLE are maintained by the Office of the General Counsel.

2. Information that is retained by the FFC may be considered active intelligence or criminal investigative information and, therefore, is exempt from public disclosure. When there is legal basis for denial, the existence, content, and source of the information will not be made available to an individual. To the extent allowed by law, information will not be verified or released if:
   - the disclosure would interfere with, compromise, or delay an ongoing investigation;
   - the disclosure would endanger the health or safety of an individual, organization, or community; or
   - the information is deemed active criminal intelligence information or active criminal investigative information.

3. If FDLE is not the original source of the information about which the public records request has been made, the original source agency will be contacted by FDLE for appropriate response to said request. If a public records request was made through the FDLE and the decision was made to release information, any complaints or objections to the accuracy or completeness of information retained about him or her should be made in writing and handled through the FFC Privacy Officer. The individual would be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. The information would then be submitted to the FDLE for consideration.

4. The individual to whom information has been disclosed will be provided with a justification and the opportunity for an appeal if the request for correction is denied by the FFC. Upon denial, the individual will be informed of the methods for correcting or modifying the information, if available. All appeals with be handled by the FDLE Office of General Counsel, in consultation with the Office of Inspector General. A record will be kept of all requests and of what information is disclosed to an individual.

5. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information resulting in specific, demonstrable harm to said individual, and that such information about him or her is alleged to be held by the FFC, the FFC**,** must inform the individual how to submit complaints or request corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any. Should it be deemed appropriate, FDLE and the FFC will assist the originating agency upon request in correcting, purging or clarifying any identified data/record deficiencies identified in the public records request.

6. The FFC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of any ISE-SAR or information provided to the ISE that contains information in privacy fields that identifies the individual. However, any personal information will be reviewed and corrected or deleted if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

    - A designated member of the FDLE Office of General Counsel serves as the FFC Privacy Officer. The FFC Director will assist the Privacy Officer in determining whether complaints involve information that has been submitted to the ISE or is

otherwise in the possession of the FFC. A written record of complaints including information which has been provided to the ISE will be maintained by the FFC Director and shall be made available for additional action as appropriate. The FFC will provide written notice to receiving ISE entities of information it has received from the FFC that is in need of redress.

- The Privacy Officer will regularly consult with experts in the fields of privacy, civil rights, and civil liberties on evolving best practices, public considerations, and legal updates. Such experts may include other fusion center legal advisors and privacy officers, federal government P/CRCL advisers, and non-governmental experts. The Privacy Officer will also conduct Privacy Impact Assessments on any new initiatives, tools, and technologies that may reasonably collect PII.

P. Security Safeguards

1. The FFC Director has designated an FDLE member to serve as the security officer who shall receive appropriate training and shall support the security needs of the FFC.

2. The FFC will operate in a secure facility, protecting it from external intrusion. The FFC will utilize secure internal and external safeguards against network intrusions, to include intelligence system records. Access to FFC databases and reporting systems from outside the facility will only be allowed over secure networks.

3. The FFC 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.

4. Access to FFC information will only be granted to FFC members whose position and job duties require such access and who have successfully completed a background check and appropriate security clearance, if applicable, and those who have been selected, approved, and trained accordingly.

5. Queries made to the FFC data applications will be logged into the data system identifying the user initiating the query. The FFC will utilize watch logs to maintain audit trails of requested and disseminated information.

6. The FDLE has stringent physical, procedural and technical security safeguards that govern the security of data systems administered by the FDLE and accessed by FFC and FDLE members. The following operational security issues are addressed by FDLE policies 2.5, 2.6, 2.7, 2.8 and 2.11:
    - Confidentiality of data and information
    - Control of computers and information resources
    - Physical security and access to data processing facilities
    - Logistical and data access controls/data and system integrity
    - Network security
    - Backup and recovery
    - Personnel security and security awareness
    - Systems acquisition, auditing and reporting
    - Information technology resource standards
    - Software management and accountability
    - Password management
    - Security of mobile devices

As the FFC falls under the administration and authority of the FDLE, these policies are applicable to and govern FFC operations. The FFC will, in the event of a data security breach, comply with all applicable state and federal laws regarding notification to compromised individuals.

Q. Information Retention and Destruction

1. All criminal intelligence information will be reviewed for record retention (validation or purge) at least every five (5) years, as required by 28 CFR Part 23. When information has no further value or meets the criteria for removal according to FDLE Policy 1.15 and the FFC retention and destruction policy, and according to applicable law, it will be purged and/or returned to the contributing agency. Each contributor is responsible for its compliance with applicable public records laws, as well as the records retention and destruction rules and guidelines of the Department of State.

2. The FFC will retain ISE-SAR information in the designated reporting system for a sufficient period of time to permit the information to be validated or refuted, its credibility and value to be reassessed, and to the degree possible, a "disposition" label will be assigned so that subsequent authorized users know the status and purpose for the retention.

3. All SAR information, tips, and leads contained in the designated Florida statewide intelligence system and contributed to the designated national system by the FFC will be reviewed no later than 90 days after entry to make a determination of its status. SARs, tips, and leads that are determined not to be valid will be purged from the system. SARs, tips, and leads that are unsubstantiated will be purged as soon as permissible pursuant to applicable Florida Department of State retention schedules.

4. The retention or classification of existing information will also be re-evaluated whenever:
   - New information is added that has an impact on access limitations, the sensitivity of disclosure, or confidence in the information;
   - There is a change in the use of the information affecting access or disclosure limitations; or,
   - Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

R. Information System Transparency

1. The FFC will be transparent with the public in regard to information and intelligence collection practices. The FFC's Privacy Policy will be provided to the public for review via the FDLE public website.

2. The FFC Privacy Officer will be responsible for receiving and coordinating a response to inquiries and complaints about privacy, civil rights, and civil liberties protections related to ISE-SAR information and the operations of the FFC.

S. Accountability

1. The FFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in accordance with this policy and applicable law. These procedures will be incorporated into the FFC Standard Operational Procedures.

2. The FFC will have access to records of inquiries to and information disseminated from the ISE platforms.

   An audit log of queries will identify the user initiating the query. This will include periodic and random audits of logged access to the designated national suspicious activity reporting system in accordance with audit obligations within the ISE-SAR policy or as otherwise utilized by the FFC Privacy Officer.

3. The FFC Privacy Officer will conduct annual audits of the criminal intelligence systems maintained and controlled by the FFC and report results and recommendations to the FFC Director. Records of audits will be maintained by the Privacy Officer or their designee. Any audits conducted will be in such a manner as to protect the confidentiality, sensitivity, and privacy of records and/or reports of audits, as well as any related documentation.

4. The members of the FFC may report violations or suspected violations of the Privacy Policy to the FFC Privacy Officer or any supervisor.

5. If an authorized user is found to have violated the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the FFC may**,** in consultation with the FDLE Office of General Counsel, the FDLE Inspector General, or the Office of Executive Investigations, as appropriate:
   - Suspend or discontinue access to information by the user;
   - Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
   - Apply administrative actions or sanctions as provided by rules and regulations or as provided in agency personnel policies;
   - If the user is from an agency external to the FDLE, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

6. The FFC Director, in consultation with the FFC Privacy Officer, will annually review and provide guidance, as appropriate, on the provisions protecting privacy, civil rights, and civil liberties contained within this policy and provide guidance on appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

T. Enforcement

The FFC reserves the right of access to FFC information and to suspend or withhold service to any personnel violating the Privacy Policy. The FFC reserves the right to deny access to systems, FFC products or ISE-SAR information to any participating agency or individual user who fails to comply with the applicable restrictions and limitations of the FFC Privacy Policy.

U. Training

1. All participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to the designated Florida statewide intelligence system will participate in training programs

regarding implementation of and adherence to privacy, civil rights and civil liberties policies and protections pertinent to the scope of their employment and access to said information.

2. All FFC members, are required to attend training regarding privacy, civil rights and liberties as determined by the Special Agent in Charge of OSI and the FFC Director. These trainings will include the following:
   - Purpose of the Privacy Policy;
   - Substance and intent of the provisions of the policy relating to the collection, use, analysis, retention, destruction, sharing and disclosure of information;
   - How to implement the policy in the day-to-day work of a participating agency;
   - The impact of improper activities associated with violations of the policy;
   - Mechanisms for reporting violations of the policy;
   - The possible penalties for policy violations, to include criminal liability.