SEFFC ISE-SAR EE PRIVACY POLICY

SOUTHEAST FLORIDA FUSION CENTER

ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights and Civil Liberties Protection Policy

The Miami-Dade Police Department's Homeland Security Bureau is a Fusion Center (herein referenced to as MDPD, HSB, or SEFFC) as defined below:

MISSION STATEMENT:

The Mission of the MDPD's HSB/SEFFC is to enhance partnerships, which foster a connection between every facet of the law enforcement community. HSB will afford the men and women, who are dedicated to protecting the public and addressing violence, with all available intelligence resources and communications capabilities. Unless readily shared, critical information is without value.

HSB's criminal intelligence products and services will be made available to law enforcement agencies and other criminal justice entities with a demonstrated right and need to know. All agencies who participate in HSB will be subject to a Memorandum of Understanding and will be required to adhere to all HSB's policies and security requirements. The purpose of this Privacy Policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged.

All Center personnel will comply with all state, local and federal laws protecting privacy, civil rights and civil liberties and adhere to the guidelines set forth in 28CFR Part 23. HSB will provide a printed copy of this policy to all departmental and non-departmental personnel who provide services and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

A. Purpose Statement

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

1. The purpose of the Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR) Evaluation Environment Initiative (hereafter "EE Initiative") Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy and CR/CL Policy") is to promote SEFFC or "submitting agency"), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct under the EE Initiative that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists participants in:
   - Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
   - Increasing public safety and improving national security.
   - Minimize the threat and risk of injury to citizens.
   - Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.

- Minimize the threat and risk of danger to real or personal property.
- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to public safety agencies.
- Minimize reluctance of individuals or groups to use or cooperate with the justice system.

GUIDING PRINCIPLES:

HSB's Privacy Policy has eight Privacy Design Principles, which shall guide the policy and practices wherever applicable. The eight Privacy Design principles are:

1. **Purpose Specification** – Define the HSB's purpose for information to help ensure the agency uses of information is appropriate.
2. **Collection Limitation** – Limit the collection of personal information to that required for the purposes intended.
3. **Data Quality** – Ensure data accuracy
4. **Use Limitation** – Ensure appropriate limits on Department use of personal information.
5. **Security safeguards** – Maintain effective security over personal information
6. **Openness** – Maintains a citizen's access to information available through the Freedom of Information Act.
7. **Individual Participation** – Allow individual's reasonable access and opportunity to correct errors in their personnel information held by the agency.
8. **Accountability** – Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

B. Policy Applicability and Legal Compliance

1. All participating SEFFC personnel (including personnel providing information technology services to the SEFFC), private contractors, and other authorized participants will comply with applicable provisions of the SEFFC's Privacy and CR/CL Policy concerning personal information, including:
   - SAR information the source agency collects and the SEFFC receives.
   - The ISE-SAR information identified, submitted to the shared space, and accessed by or disclosed to SEFFC personnel.

2. The SEFFC will provide a printed copy of its Privacy and CR/CL Policy to all SEFFC personnel, non-agency personnel who provide services to the SEFFC and to each source agency and SEFFC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with applicable provisions of this policy.

3. All SEFFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution, Florida Constitution's Declaration of Rights, as well as state, local, and federal privacy, civil rights, civil liberties, and legal requirements applicable to the SEFFC and/or other participating agencies. (See, Appendix B, detailing Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information.)

C. Governance and Oversight

1. The SEFFC Intelligence Analyst Supervisor/Sergeant of the SEFFC will have primary responsibility for operating the SEFFC, ISE-SAR information system operations, and coordinating personnel involved in the EE Initiative; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR and ISE-SAR information; and enforcing the provisions of this policy.

2. The Privacy and CR/CL Policy is guided and updated annually through recommendations made by an agency-designated privacy committee that liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the agency's/center's information collection, retention, and dissemination processes and procedures.

3. The SEFFC's participation in the EE Initiative will be guided by a trained Privacy Officer who is appointed by the SEFFC Director to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy.

D. Terms and Definitions

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

E. Information

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

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

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

3. Upon receipt of SAR information from a source agency that has processed the information in accordance with SEFFC criteria (business processes), designated SEFFC personnel will:
   - Personally review and vet the SAR information and provide the two-step assessment set forth in the ISE-SAR Functional Standard (FS) to determine whether the information qualifies as an ISE-SAR (alternatively, SEFFC personnel may confirm that such an assessment has been conducted by an authorized source agency).
   - Enter the information following Information Exchange Package Documentation (IEPD) standards and code conventions to the extent feasible.
   - Provide appropriate labels as required under E.5 and E.6 below.
   - Submit (post) the ISE-SAR to the SEFFC's shared space.
   - Notify the source agency that the SAR has been identified as an ISE-SAR and submitted to the shared space.

4. The SEFFC will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:
   - The name of the source agency.
   - The date the information was submitted.
   - The point-of-contact information for SAR-related data.
   - Information that reflects any special laws, rules, or policies regarding access, use, and disclosure.

5. Information provided in the ISE-SAR shall indicate, to the maximum extent feasible and consistent with the ISE FS, SAR Version 1.0 (ISE-FS-200):
   - The nature of the source: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source.
   - Confidence, including:
     The reliability of the source:
     - Reliable—the source has been determined to be reliable.
     - Unreliable—the reliability of the source is doubtful or has been determined to be unreliable.
     - Unknown—the reliability of the source cannot be judged or has not as yet been assessed.

     The validity of the content:
     - Confirmed—information has been corroborated by an investigator or other reliable source.
     - Doubtful—the information is of questionable credibility, but cannot be discounted.
     - Cannot be judged—the information cannot be confirmed.
   - Unless otherwise indicated by the source or submitting agency, source reliability is deemed "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or validate it through their own investigation.
   - At all times, due diligence will be exercised in determining source reliability and content validity. In accordance with Section L, Information Retention and Destruction, and record retention as provided by Section 23.20 (h) of 28 CFR Part 23, information determined to be unfounded will be purged from the shared space.
   - Notwithstanding Section L, Information Retention and Destruction, and record retention as provided by 28 CFR Part 23, information determined to be unfounded will be purged from the shared space.

6. At the time a decision is made to post ISE-SAR information to the shared space, SEFFC personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the ISE-SAR FS, to reflect any limitations on disclosure, based on sensitivity of disclosure (dissemination description code), in order to:
   - Protect every natural person's right to privacy, civil rights, and civil liberties.
   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Provide any legally required protection based on an individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

7. The SEFFC will share ISE-SAR information with authorized non-fusion center agencies and individuals only in accordance with established SEFFC policy and procedure.

8. The SEFFC will ensure that ISE-SAR information in the shared space that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will be updated (replaced) to so indicate. Information determined to be unfounded will be purged from the shared space.

9. The classification of existing information will be reevaluated whenever 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.

10. The SEFFC will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR and ISE-SAR information (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as the privacy, civil rights, and civil liberties of individuals.

11. Notice will be provided through data field labels or narrative information, which will clearly indicate any legal restrictions on information sharing based on information sensitivity or classification, and thus enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

F. Acquiring and Receiving Information

1. Information acquisition and investigative techniques used by source agencies must comply with and adhere to applicable law, regulations, and guidelines, including, where applicable, U.S. and state constitutional provisions, applicable federal and state law provisions, and local ordinances and regulations.

2. The SEFFC will not directly or indirectly receive, seek, accept, or retain information from an individual, nongovernmental entity or information provider that is legally prohibited from obtaining or disclosing the information.

3. Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the SEFFC are governed by the laws and rules governing those individual agencies, as well as applicable federal and state laws and will be trained to recognize behavior that is indicative of criminal activity related to terrorism.

4. When a choice of investigative techniques is available, information documented as a SAR or ISE-SAR 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.

5. Access to and use of ISE-SAR information is governed by the U.S. Constitution, the Constitution of the State of Florida, applicable federal and state laws, and local ordinances, and Office of the Program Manager for the Information Sharing Environment (PM-ISE) policy guidance applicable to the ISE-SAR EE initiative.

G. Information Quality Assurance

1. The SEFFC will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the SEFFC. The SEFFC will advise the appropriate contact person in the source agency, in writing (this would include electronic notification), if SAR information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

2. The SEFFC will make every reasonable effort to ensure that SAR information collected and ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy source agencies and is as accurate, current, and complete as possible.

3. At the time of posting to the shared space, ISE-SAR information will be labeled according to the level of confidence in the information (source reliability and content validity) to the maximum extent feasible.

4. The labeling of ISE-SAR information will be periodically evaluated and updated in the shared space when new information is acquired that has an impact on confidence in the information.

5. Alleged errors or deficiencies (misleading, obsolete, or otherwise unreliable) in ISE-SAR information will be investigated in a timely manner and any needed corrections to or deletions made to such information in the shared space are completed.

6. ISE-SAR information will be removed from the shared space if it is determined the source agency did not have authority to acquire the original SAR information, used prohibited means to acquire it, or did not have authority to provide it to the SEFFC or if the information is subject to an expungement order in a state or federal court that is enforceable under state law or policy.

7. The SEFFC will provide written notice (this would include electronic notification) to the source agency that provided the SAR and to any user agency that has accessed the ISE-SAR information posted to the shared space when the ISE-SAR is corrected or removed from the shared space by the SEFFC because it is erroneous or deficient such that the rights of an individual may be affected.

H. Analysis

ISE-SAR information posted by the SEFFC to the shared space or accessed from the shared spaces under the EE Initiative will be analyzed for intelligence purposes only by qualified SEFFC personnel who; have successfully completed a background check and any applicable security clearance; and have been selected, approved, and trained accordingly (including training on the implementation of this policy). These personnel shall share ISE-SAR information only through authorized analytical products.

8. ISE-SAR information is analyzed according to priorities and needs, including analysis, to:
   - Further terrorism prevention, investigation, force deployment, or prosecution objectives and priorities established by the SEFFC.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in terrorism-related activities.

I. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used, as appropriate, to determine which system users will be authorized to view privacy fields in ISE-SAR information in response to queries made through a federated ISE-SAR search.

2. Unless an exception is expressly approved by the PM-ISE, the SEFFC will adhere to the FS for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, EE Initiative-approved data collection codes, and ISE-SAR information sharing and disclosure business rules.

3. ISE-SAR information retained by the SEFFC and entered into the SEFFC's shared space will be accessed by or disseminated only to persons within the SEFFC or, as expressly approved by the PM-ISE, users who are authorized to have access and need the information for specific purposes authorized by law. Access and disclosure of personal information will be allowed to agencies and individual users only for legitimate law enforcement and public protection purposes and for the performance of official duties in accordance with law.

4. ISE-SAR information posted to the shared space by the SEFFC may be disclosed to a member of the public **only if** the information being sought:
   a. Is a matter of public record pursuant to Section 24(a), Article I, of the Constitution of the State of Florida, and Chapter 119, Florida Statutes; and
   b. Not exempt pursuant to Chapter 119, Florida Statutes; or
   c. Otherwise, appropriate for release to further the SEFFC mission.

   Such information may be disclosed only in accordance with the law and procedures applicable to the SEFFC for this type of information.

5. ISE-SAR information will not be provided to the public if, pursuant to Chapter 119, Florida Statutes, it is:

   - Required to be kept confidential or exempt from disclosure.
   - Classified as criminal intelligence or criminal investigative.
   - Protected federal, state, or tribal records originated and controlled by the source agency that cannot be shared without permission.
   - A violation of an authorized nondisclosure agreement. (if not superseded by Chapter 119, Florida Statutes)

6. The SEFFC will not confirm the existence or nonexistence of ISE-SAR information to any person, organization, or other entity not otherwise entitled to receive the information.

J. Disclosure and Correction/Redress

J.1. Mandatory Disclosure and Correction

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in item 2 listed below, an individual who is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the SEFFC or a source agency participating in the EE Initiative, may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The SEFFC's response to the request for information will be made in compliance with disclosure under Chapter 119, Florida Statutes. A record will be kept of all requests and of what information is disclosed to an individual.

2. The existence, content, and source of the information will not be made available to an individual when such discloser violates Chapter 119, Florida Statutes.

3. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the SEFFC or the source agency. The individual will also be informed of the procedure for appeal when the SEFFC or source agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

J.2. Redress (complaint and correction when no right to disclosure)

1. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the SEFFC, the SEFFC, as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

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

K. Security Safeguards

1. The SEFF's Executive Officer, or designee, is designated and trained to serve as the SEFFC's security officer for the EE Initiative.

2. The SEFFC will operate in a secure facility that is protected from external intrusion. The SEFFC will utilize secure internal and external safeguards against network intrusions of ISE-SAR information. Access to the SEFFC's ISE-SAR shared space from outside the facility will be allowed only over secure networks (LEO, HSIN, and RISSNET).

3. The SEFFC will secure ISE-SAR information in the SEFFC's shared space in such a manner that it cannot be added to, modified, accessed, destroyed, or purged except by SEFFC personnel authorized to take such actions.

4. Access to ISE-SAR information will be granted only to SEFFC personnel, whose positions and job duties require such access; who have successfully completed a background check and any applicable security clearance; and who have been selected, approved, and trained accordingly.

5. The SEFFC will, in the event of a data security breach, consider notifying an individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access, which threatens physical, reputation, or financial harm to the person. Any 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 breach or any measures necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system. Alternatively, the SEFFC may follow the breach notification guidance set forth in Office of Management and Budget (OMB) Memorandum M-07-16 (May 2007).

L. Information Retention and Destruction

1. The SEFFC will ensure that all ISE-SAR information is reviewed for record retention at least every 5 years (validation or purge) as provided by 28 CFR Part 23, and in accordance with any more restrictive time period(s) specified by state law or local ordinance. The SEFFC will also follow the provisions of Section E, Information, paragraphs 5 and 8 of this policy.

2. In accordance with Section L, paragraph 1, validation or purge, the SEFFC will maintain a record of all information to be reviewed for record retention, and when appropriate, notice will be provided to the entity submitting the information at least 30 days prior to the required review and validation/purge date. All information or records will be destroyed if the relevant information is not validated within the specified time period in accordance with applicable federal or state law, local ordinance, or SEFFC policy.

3. The SEFFC will retain ISE-SAR information in the shared space for a sufficient period of time to permit the information to be validated or refuted by trained personnel, assessed for its credibility, and to the degree possible a "disposition" label assigned so that a subsequent authorized user knows the status and purpose for the retention and thus retain the information based on any retention period associated with the disposition label.

4. When ISE-SAR information has no further suspicious activity value or usefulness and/or meets the SEFFC's criteria for purge according to applicable law or policy, privacy field information, at a minimum, will be purged.

M. Transparency, Accountability, and Enforcement

M.1. Information System Transparency

1. The SEFFC will be open with the public in regards to SAR collection and ISE-SAR information policies and practices. The SEFFC is encouraged to make the SEFFC's EE Initiative Privacy Policy available upon request and post it on the SEFFC's Web site.

2. The SEFFC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections relating to ISE-SAR information.

M.2. Accountability

1. The audit log of queries for ISE-SAR information will identify the user initiating the query.

2. The SEFFC will have access to an audit trail of inquiries to and information disseminated from the shared spaces.

3. The SEFFC will adopt and follow procedures and practices to evaluate the compliance of its authorized users with ISE-SAR information policy and applicable law. This will include periodic and random audits of logged access to the shared spaces in accordance with EE Initiative policy. Record of the audits will be maintained by the SEFFC.

4. SEFFC personnel and source agencies shall report violations or suspected violations of the SEFFC's ISE-SAR EE Initiative Privacy Policy to the SEFFC's Executive Officer.

5. The SEFFC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space. The audit will be conducted by SEFFC Intelligence Analyst Supervisor/Sergeant. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the ISE-SAR information maintained by the SEFFC in the shared space and any related documentation.

6. The SEFFC's Executive Officer as the Privacy Officer, along with a Police Legal Advisor, upon recommendations made by privacy committee (see C.2.) will annually review the SEFFC's EE Initiative Privacy Policy, and the SEFFC will make appropriate changes in response to changes in applicable law.

M.3. Enforcement

1. The SEFFC reserves the right to restrict the qualifications and number of user agencies and authorized user agency personnel that it certifies for access to ISE-SAR information and to suspend or withhold service to any of its user agencies or authorized user agency personnel violating this privacy policy. The SEFFC further reserves the right to deny access or participation in the EE Initiative to its participating agencies (source or user) that fail to comply with the applicable restrictions and limitations of the SEFFC's privacy policy.

N. Training

1. The following individuals will participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the SEFFC.
   - Personnel providing information technology services to the SEFFC.
   - Staff in other public agencies or private contractors, as appropriate, providing SAR and ISE-SAR information technology or related services to the SEFFC.
   - Source agency personnel providing organizational processing services for SAR information submitted to the SEFFC.
   - User agency personnel and individuals authorized to access ISE-SAR information who is not employed by the SEFFC or a contractor.

2. The SEFFC's privacy policy training program will cover:
   - Purposes of the EE Initiative Privacy Policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR and ISE-SAR information maintained or submitted by the SEFFC to the shared space.
   - 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, including transfer, dismissal, and criminal liability, if any.

Your signature below on this Information Sharing Environment-Suspicious Activity Report (ISE-SAR) Evaluation Environment (EE) Initiative Participation Agreement represents that you have read this agreement carefully and understand your obligation under it.

_____ _____

Source Agency Source Agency Director

Please fax, or email this page to: 305-470-3895, or ioc@mdpd.com.

Appendix A—Terms and Definitions

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

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Accountability—When a query is made to any of the SEFFC's data applications, the original request is automatically logged by the SEFFC's Intelligence Analysis Supervisor or the Sergeant into the log system**,** which will identify the user initiating the query. When such information is disseminated outside the agency from which the original request is made, a second dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for law enforcement investigative purpose or other agencies as provided by law. The agency from which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:

1. Date of release.
2. To whom the information relates
3. To whom the information was released (including address and telephone number)
4. All identification numbers or other indicator that clearly identifies the data released.
5. The purpose for which the information was released.

The MDPD will be responsible for conducting or coordinating audits and investigating misuse of data information. All violations and/or exceptions shall be reported to the MDPD's HSB/SEFFC. Individual users of the SEFFC's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use of limitations for the use of SEFFC's data may result in the suspension or termination of used privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the Center is required to abide by this Privacy Policy in the use of information obtained by and through the Center.

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

Agency—The SEFFC and all agencies that access, contribute, and share information in the SEFFC's system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Center—Center refers to the SEFFC.

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

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

Collection Limitation— SEFFC is maintained for the purposes of developing information and criminal intelligence by agencies who participate in the Center. The decision of an agency to participate in Center and which databases provide information is voluntary. Information obtained and disseminated by a law enforcement agency outside of Miami-Dade will be governed by that agency's local, state, and federal laws, as well as their respective policies.

Because the laws, rules or policies governing information and criminal intelligence that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Therefore, each contributor of information is under different legal restraints and restrictions. Each agency has its own responsibility to abide by the collection limitations applicable to it by reasons of law. Information contributed to the center should be that which has been collected in conformance with those limitations and has been vetted for legal sufficiency.

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

Data—Elements of information.

Data Quality—The agencies participating with the SEFFC retain proprietary rights (ownership) over the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data. Each contributor or contributing agency is solely responsible for data accuracy and quality.

The provisions set forth in this Privacy Policy will be reviewed annually during the first month of the year.

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

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

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

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

Members of the public cannot access individually identifiable information, on themselves or others, from the SEFFC's applications. 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. Participating agencies agree that they will refer request related to privacy or sunshine laws back to the originator of the information.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data tips and leads data, suspicious activity reports, and criminal intelligence information.

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

ISE-SAR—A suspicious activity report that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

ISE-SAR Information Exchange Package Documentation (IEPD)—A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

(1) The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.

(2) The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

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

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

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

Openness—It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative or intelligence activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

SEFFC is a collection of various databases, which allows the Department and participating agencies to share information and to accelerate the dissemination of information already collected. SEFFC does not change or alter a citizen's rightful access to information accorded to them under state law. The SEFFC complies with Florida State Statute 119 – Public Records Laws.

Participating Agencies—Participating agencies, for purposes of the EE Initiative, include source **[the agency or entity that originates SAR (and, when authorized, ISE-SAR) information]**, submitting (the agency or entity posting ISE-SAR information to the shared space), and user (an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

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

Privacy Fields—Data fields in ISE-SAR IEPDs that contain personal information.

Privacy Policy—A written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access.

The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and -implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

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

Protected Information—For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, these protections are derived from applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency.
- People or entities—private or governmental—that assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Purpose Specification—SEFFC has developed databases by using existing data sources from federal, state, and local law enforcement agencies. SEFFC will have the capability to combine data with the goal of identifying, developing, and analyzing information related to violent crime or terrorist activity for investigative leads. This capability will facilitate integration and exchange of information between participating law enforcement agencies.

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

Retention—Refer to Storage.

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

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

Use of HSB's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the HSB will be granted only to law enforcement agency personnel, sworn or non-sworn, who have been screened with a state and national fingerprint-based background check, as well as any additional background screening process using procedures and standards established by the MDPD.

The MDPD's HSB/SEFFC operates in a secure facility, protecting the HSB from external intrusion. The SEFFC will utilize secure internal and external safeguards against network intrusions. Access to HSB/SEFFC databases from outside the facility will only be allowed over secure networks.

SEFFC will store information in a manner that cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such action.

The Intelligence Section Lieutenant will serve as a security officer in addition to their regular supervisory duties. The Lieutenant will be responsible for the physical, procedural, and technical safeguards of the HSB.

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

Shared Space—A networked data and information repository, which is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing—The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency—The agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the Information Technology industry than the second meaning.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency—The agency or entity providing ISE-SAR information to the shared space.

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

Suspicious Activity Reports (SARs)—Reports that record the observation and documentation of a suspicious activity. SARs are meant to offer a standardized means for feeding information repositories. 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. 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.

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

Terrorism-Related Information—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), SARs, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or Computer Aided Dispatch (CAD) data.

A tip or lead can come from a variety of sources; including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

Training—The MDPD's HSB/SEFFC will always encourage training and provide and seek out specialized training programs for personnel assigned to the HSB. The intent of training is to develop a culture of information analysis and information sharing within the MDPD's HSB/SEFF Center.

Use Limitation—Information obtained from or through the SEFFC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

The primary responsibility for the overall operation of the MDPD's HSB/SEFFC will rest with the Major of the HSB of the MDPD. The Major, by and through the Center's Executive Officer, will enforce the Privacy Policy of the SEFFC and take the necessary measures to make certain that access to the HSB's information and resources is secure and will prevent any unauthorized access or use. The MDPD reserves the right to restrict the qualifications and number of personnel who will be accessing HSB and to suspend or withhold service to any individual violating this Privacy Policy. The Department, or persons acting on behalf of the Department, further reserves the right to conduct inspections concerning the proper use and security of the information received from the center.

Security for information derived from HSB will be provided in accordance with all applicable federal, state, and local laws, the rules, and regulations of the MDPD, and HSB policies. Furthermore, all personnel who receive, handle, or have access to HSB data and/or sensitive information will be trained as to those requirements. All personnel having access to the HSB's data agree to abide the following rules:

1. SEFFC's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer and SEFFC.
2. Individual passwords will not be disclosed to any other person except as authorized by the Department.
3. Individual passwords will be changed if authorized personnel of the Department, the SEFFC or any individual password holder suspects the password has been improperly disclosed or otherwise compromised.
4. Background checks will be completed on personnel who will have direct access to HSB.
5. Use of SEFFC's data in an unauthorized or illegal manner will subject the user to denial of further use of the SEFFC; discipline by the user's employing agency, criminal prosecution, and or civil liability.

Each authorized user understands that access to the SEFFC can be denied or rescinded for failure to comply with the application restrictions and use limitations.

User Agency—The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the shared space(s), which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

Appendix B—Legal Notes

Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the information sharing environment is explored in a key issues guidance paper titled Civil Rights and Civil Liberties Protection, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required indirectly by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the information sharing environment.

Florida's Civil liberties protections can be found in Article I, sections 1 thru 27, of Florida's Constitution; Florida Declaration of Rights. These rights are granted to all natural persons. They include the basic freedoms found in the U.S. Constitution and at times enhance privacy and other civil liberties protections. The relevant protections afforded all natural persons pursuant to the Constitution of the State of Florida are:

> **Basic rights**.--All natural persons, female and male alike, are equal before the law and have inalienable rights, among which are the right to enjoy and defend life and liberty, to pursue happiness, to be rewarded for industry, and to acquire, possess and protect property; except that the ownership, inheritance, disposition and possession of real property by aliens ineligible for citizenship may be regulated or prohibited by law. No person shall be deprived of any right because of race, religion, national origin, or physical disability.

Religious freedom.--There shall be no law respecting the establishment of religion or prohibiting or penalizing the free exercise thereof. Religious freedom shall not justify practices inconsistent with public morals, peace, or safety. No revenue of the state or any political subdivision or agency thereof shall ever be taken from the public treasury directly or indirectly in aid of any church, sect, or religious denomination or in aid of any sectarian institution.

Freedom of speech and press.--Every person may speak, write and publish sentiments on all subjects but shall be responsible for the abuse of that right. No law shall be passed to restrain or abridge the liberty of speech or of the press. In all criminal prosecutions and civil actions for defamation, the truth may be given in evidence. If the matter charged as defamatory is true and was published with good motives, the party shall be acquitted or exonerated.

Right to assemble.--The people shall have the right peaceably to assemble, to instruct their representatives, and to petition for redress of grievances.

Due process.--No person shall be deprived of life, liberty, or property without due process of law, or be twice put in jeopardy for the same offense, or be compelled in any criminal matter to be a witness against oneself.

Searches and seizures.--The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communication to be intercepted, and the nature of evidence to be obtained. This right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court. Articles or information obtained in violation of this right shall not be admissible in evidence if such articles or information would be inadmissible under decisions of the United States Supreme Court construing the 4th Amendment to the United States Constitution.

Right of privacy.--Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

Access to public records

The applicable provisions of law requiring disclosure in Florida can be found in Section 24(a), Article I, of the Constitution of the State of Florida, and Chapter 119, Florida Stat. (2008).