



**MAINE STATE POLICE
MAINE INFORMATION & ANALYSIS CENTER
PRIVACY POLICY**

TABLE OF CONTENTS

PART		PAGE
I.	Mission Statement & Guiding Principles of the Maine Information and Analysis Center	2
II.	Governance of the MIAC	2
III.	Policy Applicability	3
IV.	Definitions	4
V.	Information Management & Security	7
VI.	Information Quality	12
VII.	Collation & Analysis of Information	14
VIII.	Sharing & Disclosure of Information	15
IX.	Information Retention & Destruction	19
X.	Accountability & Enforcement	20
XI.	Training	22

Part I. Mission Statement & Guiding Principles of the Maine Information and Analysis Center

Mission Statement

1. The mission of the Maine Information and Analysis Center (MIAC) is – for criminal justice, National security, and public safety purposes only – to seek, acquire, and receive information, analyze such information, and, when lawful and appropriate, retain and disseminate such information to individuals and agencies permitted access to the information.

Guiding Principles

2. In carrying out its work, the MIAC shall endeavor:
 - A. To protect privacy, civil rights, civil liberties, and other protected interests of all individuals;
 - B. To minimize the threat and risk of injury to specific individuals or groups;
 - C. To minimize the threat and risk of damage to real or personal property;
 - D. To minimize the reluctance of individuals or groups to use or cooperate with the justice system;
 - E. To promote governmental legitimacy and accountability;
 - F. To support the role of the justice system in society;
 - G. To protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
 - H. To minimize the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health;
 - I. To increase public safety and improve national security; and
 - J. To comply with laws protecting privacy, civil rights, and civil liberties.

Part II. Governance of the MIAC

MIAC Director

1. Primary responsibility for the operation of the MIAC, the MIS, operations, coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy is assigned to the MIAC Director.
2. The MIAC Director may be contacted at the following address: intel.msp@maine.gov, attention “MIAC Director.”

MIAC Privacy Officer

3. The MIAC Director has appointed a MIAC Privacy Officer to assist in the development and review of this policy and assist with implementing the requirements of this policy.

-
4. The MIAC Privacy Officer shall be trained as described in Part XI of this policy.
 5. The MIAC Privacy Officer is to be responsible for –
 - A. Appropriate community outreach;
 - B. Ensuring that privacy and civil rights are protected as provided in this policy and by the center’s information gathering and collection, retention, and dissemination processes and procedures;
 - C. Receiving reports regarding alleged errors and violations of the provisions of this policy;
 - D. Receiving and coordinating complaint resolution under the center’s redress policy; serving as the liaison for the ISE;
 - E. Ensuring, in conjunction with the MIAC Compliance Officer, that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies;
 - F. Annually reviewing and recommending updates to this policy to the MIAC Advisory Board and the Director in response to changes in law and implementation experience, including the results of audits and inspections; and
 - G. Receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the MIS.
 - (1.) Prior to responding, the MIAC Privacy Officer may confer with Maine State Police counsel and/or the Maine Department of the Attorney General.
 6. The MIAC Privacy Officer shall ensure that enforcement procedures and sanctions outlined in this policy are adequate and enforced.
 7. The MIAC Privacy Officer may be contacted at the following address: intel.msp@maine.gov, attention “MIAC Privacy Officer.”

MIAC Compliance Officer

8. The MIAC Director shall appoint a MIAC Compliance Officer. The MIAC Compliance Officer shall conduct and coordinate audits of the center, as well as investigate, in consultation with the Privacy Officer, suspected or known misuse of information in the custody of the MIAC and suspected or known misuse of the MIS.
9. The MIAC Compliance Officer may be contacted at the following address: intel.msp@maine.gov, attention “MIAC Compliance Officer.”

MIAC Advisory Board

10. In order to ensure that the individual privacy, civil rights, and civil liberties of all individuals, remain protected, the administration of the MIAC shall be advised by a MIAC Advisory Board, which shall be responsible for reviewing new and revised policies and procedures of the MIAC and liaising with the community.

Part III. Policy Applicability

1. This policy applies to all authorized MIAC personnel, participating agency personnel, information-technology services support personnel, contractors, and other users of the

MIS. This policy applies to information in the custody and control of the MIAC that the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

2. MIAC personnel, participating agency personnel, information-technology services support personnel, contractors, and other authorized users are to endeavor to protect individuals' rights as granted by the United States of America and Maine Constitutions and other applicable law protecting privacy, civil rights, and civil liberties.¹
3. The MIAC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, those listed in footnote 1.
4. The MIAC shall provide access to an electronic copy of this policy to all individuals who are subject to the policy and to anyone requesting such access.
5. This policy will be able to be accessed worldwide via the Internet.

Part IV. Definitions

1. As used in this policy, unless the context expressly indicates otherwise, the words and terms listed in this section have the following meanings.
 - A. Acquisition. For purposes of the ISE, "acquisition" means the method by which an ISE participant obtains information through the exercise of its authorities, but does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.
 - B. Authorized. "Authorized" means formally approved by the MIAC or in accordance with law.
 - C. Center. "Center" means the Maine Information & Analysis Center (MIAC).
 - D. Civil liberties. "Civil liberties" means 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

¹ Statutory civil rights protections established pursuant to the U.S. Constitution may, in addition, directly govern State action. These include, but are not limited to, 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. The U.S. Constitution, Federal laws, Executive Orders, regulations, and policies, including, but not limited to, 28 CFR Part 23 and the Health Insurance Portability and Accountability Act (HIPAA), may potentially affect the sharing of information, including sharing terrorism-related information in the ISE. In addition to the Maine Constitution, MIAC personnel shall also adhere to the Maine Criminal History Record Information Act (16 MRSA c. 3, sub-c. 8) and Maine law regarding the interception of wire and oral communications (*see* 15 MRSA c. 102).

-
- affirmative) government action, while the term “civil liberties” involves restrictions on government.
- E. Civil rights. “Civil rights” is a term used to imply that the State has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.
 - F. Contractor. “Contractor” means any person working for the MIAC on a contractual basis who, by virtue of his or her work, shall have direct, authorized access to the MIS.
 - G. Criminal intelligence information. “Criminal intelligence information” means information or data that has been evaluated to determine that it is relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity, and meets criminal intelligence system submission criteria, as set forth in 28 CFR Pt. 23.
 - H. Information. “Information” means any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists that is collected, acquired, maintained, accessed, disclosed, and disseminated by the MIAC directly and exclusively. Information received by law enforcement agencies can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information. Information disseminated by the MIAC through means other than the MIS, e.g., RISS network systems or databases, is regulated by the laws, regulations, and policies applicable to such systems.
 - I. Information sharing environment (ISE). “Information Sharing Environment” (ISE) means a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of State, local, and Tribal agencies; Federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.
 - J. Information-technology services support personnel. “Information-technology services support personnel” means any State of Maine employee or contractor assigned to provide direct information technology services support for the MIS.
 - K. 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 crime or the security of the United States, 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.
- L. MIAC personnel. “MIAC personnel” means any person employed or contracted by the State of Maine who is assigned to the MIAC, and is either working in the MIAC physically or has direct, authorized access to the MIS.
- M. MIAC information systems (MIS). “MIAC information systems” (MIS) means electronic records, information, and databases in the custody of the MIAC that are maintained and administered exclusively by the center.
- N. Need to know. “Need to know” means, as a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual’s official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.
- O. Participating agency personnel. “Participating agency personnel” means any person working for a participating agency.
- P. Participating agency. “Participating agency” means an agency of local, county, State, Federal, or other governmental unit that exercises law enforcement or criminal investigation authority and that is formally authorized to submit and receive information to and from the MIAC.
- Q. Personally identifying information (PII). “Personally identifying information” (PII) means 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.
- R. Protected information. “Protected information” means personally identifying information about individuals that is subject to information privacy or other legal protections under the Constitution and laws of the United States and the State of Maine. Protection may be extended to organizations by Federal or Maine law, regulation, or executive order or the terms of the MIAC Privacy Policy.
- S. Public record. “Public record” means “any written, printed or graphic matter or any mechanical or electronic data compilation from which information can be obtained, directly or after translation into a form susceptible of visual or aural comprehension, that is in the possession or custody of an agency or public official of this State or any of its political subdivisions, or is in the possession or custody of an association, the membership of which is composed exclusively of one or more of any of these entities, and has been received or prepared for use in connection with the transaction of public or governmental business or contains information relating to the transaction of public or governmental business,” except as provided in the Maine Freedom of Access Act. See 1 MRSA § 402(3) & (3-A).
- T. Right to know. “Right to know” means, based on having legal authority or responsibility, or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counter-terrorism activity.
- U. RISS. “RISS” means the national program of regionally oriented services designed to enhance the ability of local, state, Federal, and Tribal criminal justice agencies to identify, target, and remove criminal conspiracies and activities spanning multi-jurisdictional, multi-State, and sometimes international boundaries; facilitate rapid

exchange and sharing of information among the agencies pertaining to known suspected criminals or criminal activity; and enhance coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be inter-jurisdictional in nature. The MIS does not include RISS-maintained and -administered systems.

- V. SAR process. “SAR process” means the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents.
- W. Suspicious Activity Report (SAR) information. “Suspicious Activity Report (SAR) information” means observed and documented behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.
- X. Tips and leads information or data. “Tips and leads information or data” means generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion. A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than “reasonable suspicion” and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.
- Y. Tips and leads program (T&LP).² “Tips and leads program” (T&LP) means a formalized process to manage tips and leads information or data, including, but not limited to, SAR information. T&LP includes the SAR process.
- Z. User. “User” means MIAC personnel or participating agency personnel who exchange MIAC-maintained information for lawful purposes.

Part V. Information Management & Security

1. The MIAC shall only seek, acquire, retain, or share information that:
 - A. Is based on a criminal predicate or possible threat to public safety; or

² The MIAC does not yet participate in and has not implemented a T&LP.

-
- B. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal conduct or activity that presents a threat to any individual, the community, or any nation and that the information is relevant to the criminal conduct or activity; or
 - C. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
 - D. Is useful in a crime analysis or in the administration of criminal justice and public safety; and
 - E. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
 - F. The information was collected in a fair and lawful manner.
2. The MIAC may retain information that is based on a level of suspicion that is less than “reasonable suspicion,” such as tips and leads or SAR information.
 3. The MIAC shall not intentionally seek, acquire, 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 non-criminal organization or event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.
 4. The MIAC shall document the source of all information acquired and retained by the center in accordance with this policy.

Labeling of Information

5. The MIAC shall apply labels to information to indicate to authorized users accessing the MIS that:
 - A. The information is protected information (see Part IV, “Definitions”);
 - B. The information is subject to local, State or Federal law restricting access, use, or disclosure, including, but not limited to, the Maine Freedom of Access Act (16 MRSA c. 13) and the Maine Criminal History Record Information Act (16 MRSA c. 3, sub-c. 8).
6. When receiving and analyzing information received by the MIAC, MIAC personnel shall assess the information to determine or review its nature, usability, and quality. MIAC personnel shall assign categories to the information to reflect the assessment, such as:
 - A. Whether the information consists of –
 - (1) Tips and leads data;
 - (2) SARS;
 - (3) Criminal history information;
 - (4) Intelligence information;
 - (5) Case records;
 - (6) Conditions of supervision;
 - (7) Case progress; or
 - (8) “Other information”;

-
- B. The nature of the source as it affects veracity;
 - (i) For example –
 - (a) “Anonymous tip”;
 - (b) Trained interviewer or investigator”;
 - (c) “Public record”;
 - (d) “Private sector”;
 - C. The reliability of the source;
 - (i) For example –
 - (a) “Reliable”;
 - (b) “Usually reliable”;
 - (c) “Unreliable”;
 - (d) “Unknown”;
 - D. The validity of the content –
 - (i) For example –
 - (a) “Confirmed”;
 - (b) “Probable”;
 - (c) “Doubtful”;
 - (d) “Cannot be judged.”
7. At the time a decision is made by the MIAC to retain information, the information shall be labeled to the maximum extent feasible and reasonable, and pursuant to applicable limitations on access and sensitivity of disclosure, in order to:
- A. Protect confidential sources and police undercover techniques and methods;
 - B. Not interfere with or compromise pending criminal investigations;
 - C. Protect an individual’s right of privacy or their civil rights and civil liberties;
 - D. Provide legally required protections based on the individual’s status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.
8. The labels assigned to existing information under this section shall be reevaluated whenever:
- A. New information is added that is known to have a material impact on access limitations or the sensitivity of disclosure of the information;
 - B. There is a known change in the use of the information materially affecting access or disclosure limitations (for example, the information becomes part of court proceedings for which there are different public access laws).

-
9. The MIAC will incorporate the SAR process into existing processes and systems used to manage other crime-related information and criminal intelligence.
 10. The MIAC shall attach specific labels and descriptive metadata to MIS information that shall be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

Methods of Seeking or Receiving Information

11. Information gathering and investigative techniques used by the MIAC shall comply with all applicable laws.
12. The MIAC shall not intentionally directly or indirectly receive, seek, accept, or retain information from an individual or nongovernmental information provider, commercial database, who may or may not receive a fee or benefit for providing the information, if the center knows or has reason to believe that:
 - A. The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to personnel within the center;³
 - B. The individual or information provider used methods for collecting the information that MIAC personnel could not legally use;⁴
 - C. It is known that the specific information sought from the individual or information provider could not legally be collected by any MIAC personnel; or
 - D. MIAC personnel, or participating agency personnel, have not taken steps necessary to be authorized to collect the information.
13. Information gathering and investigative techniques used by the MIAC shall be no more intrusive or broad-scale than is necessary in the particular circumstance to gather information it is authorized to seek or retain pursuant to this policy. External agencies that access MIAC information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable Federal and State laws.
14. To the extent it will do so at all, the MIAC shall contract only with commercial database entities that certify in writing (1) that their methods for gathering personally identifiable information comply with applicable local, State, Tribal, territorial, and Federal laws, statutes, and regulations, and (2) that these methods are not based on misleading information-gathering practices.

Basic Descriptive Information

15. The MIAC requires certain basic descriptive information to be entered in the MIS and electronically associated with data (or content) for which there are known to be special

³ An exception to this is if the individual did not act as an agent of or at the direction of any bona fide law enforcement officer participating with the center

⁴ An exception to this is if the individual did not act as an agent of, or at the direction of any bona fide law enforcement officer participating in the center. In this particular case, the MIAC Director shall seek the advice of the Maine State Police Staff Attorney on the current prevailing State and Federal case law on information obtained by a third party individual that is counter to laws of criminal procedure before any information is used.

laws, rules, or policies regarding access, use, and disclosure. To the extent reasonably known or ascertainable, the types of information should include:

- A. The name of the originating agency, with reasonable specificity as to the division or unit of the agency from which the information originates;
- B. The name of the agency's justice information system from which the information is disseminated;
- C. The date the information was collected and, where feasible, the date its accuracy was last verified;
- D. The title or position, and contact information of the person to whom questions regarding the information should be directed.

Received tips, leads, and SAR information

16. The center may receive tips, leads, and SAR information. When the MIAC does so, MIAC personnel are to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of such information. MIAC personnel shall:

- A. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value, and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.
 - (1) The MIAC shall use a standard reporting format and data collection codes for SAR information;
- B. Store the information using a storage method similar to that used for data that rises to the level of reasonable suspicion and includes a documentation and inspection process, supporting documentation, and labeling of the data to delineate it from other information;
- C. Allow access to or disseminate the information using a similar (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion;
 - (1) For example, "need-to-know" and "right-to-know" access or dissemination;
- D. When appropriate, provide access to or disseminate the information in response to an interagency inquiry for law enforcement, national security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property;
- E. Retain tips and leads information or data under the tips and leads program (T&LP) for one year to determine its credibility and value;

-
- F. Assign a “disposition” label to the information so that a subsequently authorized user knows the status and purpose for the retention and retain the information based on the retention period associated with the disposition label;
 - (i) For example –
 - (a) “Undetermined”;
 - (b) “Unresolved”;
 - (c) “Cleared”
 - (d) “Unfounded”; or
 - (e) “Under active investigation”;
 - G. Adhere to and follow the center’s physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information.
 - (i.) Tips, leads, and SAR information shall be secured in a manner similar to that secures data that rises to the level of reasonable suspicion is secured;
 - H. The MIAC shall make reasonable efforts to identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the ISE. Further, the center shall provide notice mechanisms, including, but not limited to, metadata or data field labels, that shall enable ISE users to determine the nature of the protected information and how to handle the information in accordance with the Department of Homeland Security classifications and applicable legal requirements.
17. The MIAC’s SAR process shall provide for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. MIAC personnel shall be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
18. The MIAC’s SAR process shall include safeguards to ensure, to the greatest degree possible, that only information regarding individuals and organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism shall be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties shall not be intentionally or inadvertently gathered, documented, processed, and shared.

Part VI. Information Quality

- 1. Information gathering (acquisition and access) and investigative techniques used by the MIAC and participating agency personnel providing information to the center are required to be in compliance with, and shall adhere to applicable regulations and guidelines, including, but not limited to:
 - A. Applicable criminal intelligence guidelines established under the U.S. Department of Justice’s (DOJ) National Criminal Intelligence Sharing Plan (NCISP);
 - B. Maine Rules of Criminal Procedures;

-
- C. 28 CFR Pt. 23 regarding criminal intelligence information.
2. The MIAC shall make every reasonable effort to ensure that information sought, acquired, and retained by the center is:
 - A. Derived from dependable and trustworthy sources of information;⁵
 - B. Accurate;
 - C. Current;
 - D. Complete (including the relevant context in which it was sought or received and other related information);⁶
 - E. Merged with other information about the same individual or organization only when the applicable standard (as set forth in Part VI of this policy) has been met.
 3. Criminal intelligence information shall include "confidence labeling" of source reliability and content validity in accordance with this policy. All criminal intelligence submissions made to the MIS shall be reviewed to ensure they meet the requirements of 28 CFR Part 23. The MIAC shall notify the user contributing the information if the information is found not to have been submitted in compliance with that Federal regulation. The MIAC shall set a deadline by which the information must be validated for a new retention period by the user or agency submitting the information. If the deadline is not met, or the user contributing the information cannot be reached in a timely manner, the information shall be discarded and deleted.
 4. At the time of inclusion in the MIS, information shall be labeled regarding its level of quality (accuracy, completeness, currency, and confidence (source reliability and content validity)). The labeling of retained information will be reevaluated by the MIAC or the originating agency when new information is gathered that has an impact on confidence in previously retained information.
 5. If MIAC or participating agency personnel have a concern, or are notified of a concern by another, regarding source reliability, or if information is in error such that it may affect a person's rights or civil liberties, the MIAC Privacy Officer shall be timely notified of the concern when the issue is discovered. The MIAC Privacy Officer shall review the allegation in accordance with Part IX of this policy.
 6. To the extent feasible, the center shall review the quality of information it receives from participating agency personnel and advise the appropriate contact person at that agency in writing if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable. Participating agency personnel are solely responsible for reviewing the quality and accuracy of the information provided to the MIAC.
 7. The MIAC Privacy Officer shall provide the MIAC Director with a written report on each source reliability investigation on which the MIAC Privacy Officer works. All content error investigations shall be documented by the MIAC.

⁵ This may include commercial databases in addition to participating agencies.

⁶ Open source information, public information, or a source with an unknown reliability may be sought, acquired, and retained by the MIAC, but shall be noted as such and a disclaimer shall be added to the information that indicates (1) that the information may not be accurate, and (2) that the recipient should independently assess and verify the content of the information before any action is taken based on the result of the source

-
8. The MIAC Director shall maintain a record of sources not in compliance with this policy to ensure they are not used by the MIAC until the issues have been resolved.
 9. The MIAC shall conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information shall be corrected, deleted from the MIS, or not used when the center identifies information that is erroneous, misleading, obsolete, or – in light of the totality of attendant circumstances – unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information.⁷
 10. MIAC personnel and the MIAC Privacy Officer shall make reasonable efforts to notify the MIAC Director that information maintained in the MIS must be corrected or deleted by the MIAC when such personnel learns and confirms that:
 - A. The information is erroneous, misleading, obsolete, unreliable, improperly merged, or lacks adequate context such that the rights of the individual may be affected;
 - B. The source of the information did not have authority to gather the information or to provide the information to the center;⁸
 - C. The source of the information used prohibited means to gather the information, except when the source did not act as an agent at to a bona fide law enforcement officer.
 11. The MIAC Director shall advise the appropriate participating agency personnel if a determination is made that information submitted by the agency needs to be corrected or deleted pursuant to applicable law or this policy.
 12. If erroneous information is provided from a commercial database, the MIAC Director, or designee, may notify the privacy office or appropriate contact of the business. The MIAC, however, shall not assume responsibility to notify the commercial entity.
 13. The MIAC shall notify recipient agencies when information previously provided to them by the MIAC is known to have been deleted or changed pursuant to this policy.
 14. Notifications made pursuant to this policy by the MIAC shall be sent in writing. The investigation shall include documentation as to the notice and when sent.
 15. The MIAC shall establish security physical and electronic safeguards to ensure that only authorized users are allowed to add, change, or delete information in the MIS.

Part VII. Collation & Analysis of Information

Collation and Analysis

⁷ Except when the center's information source did not act as the agent of the center in gathering the information.

⁸ Except when the source did not act as an agent to a bona fide law enforcement officer, and only if the rules of criminal procedure and prevailing State and Federal case laws allows it, and only after consultation with Maine State Police counsel and/or the Maine Department of the Attorney General.

-
1. Information that is sought or received by the MIAC or from other sources under Part V. shall only be analyzed for purposes consistent with this policy:
 - A. By MIAC personnel who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly;
 - B. To 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 generally; and
 - C. To further crime prevention, enforcement, force deployment, or prosecution objectives and priorities; or
 - D. For activity which may pose a threat to the public safety, including, but not limited to, the safety of law enforcement officers and criminal justice agency personnel.
 2. Information sought, acquired, or received by the MIAC or other sources shall not be intentionally analyzed or combined in a manner or for any purpose that violates this policy.

Merging of Information from Different Sources

3. Information about an individual or organization from two or more sources shall not be purposefully merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.
4. The set of identifying information sufficient to allow merging shall consist of available attributes that can contribute to higher accuracy of match, but should have at least three matches.
5. 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.

Pre-dissemination/-sharing Review of Certain MIAC-created Intelligence Products

6. To the extent time and resources permit, the MIAC Privacy Officer is to review all strategic intelligence products created by the MIAC to ensure that they provide appropriate privacy, civil rights, and civil liberties protections, before such products are disseminated or shared by the center.

Part VIII. Sharing & Disclosure of Information

1. Credentialed, role-based access criteria will be used by the MIAC, as appropriate, to control:
 - A. The information to which a particular group or class of users can have access based on the group or class;
 - B. The information a class of users can add, change, delete, or print; and
 - C. To whom, individually, the information can be disclosed and under what circumstances.

-
2. The MIAC shall adhere to the current and effective version of the *ISE-SAR Functional Standard* for the SAR process when ISE information is involved, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the standard for suspicious activity potentially related to terrorism.
 3. Information disclosed or shared by the MIAC shall be appropriately labeled.
 4. To delineate protected information shared through the ISE from other data, the MIAC maintains records of agencies sharing terrorism-related information, audit logs, and employs system mechanisms to identify the originating agency when the information is shared with the MIAC.
 5. The MIAC may disclose or share information with a validity expiration date. This date may be shorter than the retention period of the center. The label shall indicate that, after the expiration date, the information is considered obsolete, and the recipient shall be responsible for destroying their copies of the information. The center shall consider labeled documents beyond the expiration date as having met notification requirements contemplated in Part VIII of this policy.
 6. Direct access to information retained by the MIAC shall only be provided to individuals authorized to have such access.
 - A. Each such instance of access shall be manually or electronically documented.
 7. The MIS may be accessed by non-MIAC personnel only when the system is capable of providing an audit trail to the administrators in the center.
 - A. Each such instance of access shall be manually or electronically documented.
 8. Agencies external to the MIAC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

Sharing Information with Those Responsible for Public Protection, Safety, or Public Health

9. The MIAC Director may authorize information retained by the MIAC to be disseminated to individuals not subject to this policy, but strictly for the purpose of protecting the safety of those individuals and/or the public generally.
 - A. Each such instance of such dissemination shall be manually or electronically documented.

Sharing Information for Specific Purposes

10. Information gathered and retained by the MIAC may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users or purposes specified in the law.
11. The MIAC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

-
- A. Each such request, and the disposition thereof, shall be manually or electronically documented. Such documentation shall be kept for a minimum of 5 years.

Disclosing Information to the Public in the Aid of Investigation

12. Information gathered and retained by the MIAC may be disclosed to the public or media if the information is a public record, or if the release of the information, if protected, would aid of an investigation or public safety. Access to records is governed by 1 MRSA c. 13, Maine Freedom of Access Act, and 16 MRSA c. 3, sub-c. 8, Maine Criminal History Recording Information Act.
13. The MIAC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

- A. Each such disclosure shall be manually or electronically documented. Such documentation shall be kept for a minimum of 5 years.

Disclosing Information to the Individual about Whom Information Has Been Gathered

14. Upon satisfactory verification (e.g., fingerprints) of his or her identity, and subject to the conditions specified in this policy, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the MIAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The center's response to the request for information shall be made to the requesting individual by the MIAC Privacy Officer within a reasonable amount of time (thirty (30) days) and in a form that is readily intelligible to the individual. If the information did not originate with the MIAC, the requestor shall be referred to the originating agency, if appropriate or required, or the center shall notify the source agency of the request and its determination that disclosure by the MIAC or referral of the requestor to the source agency was neither required nor appropriate under applicable law. A record will be kept of all requests and of what information is disclosed to an individual.
15. Generally speaking, there are several categories of records to which the public will not be provided access. These include, but are not limited to, the following:

- A. Records required to be kept confidential by law are exempted from disclosure requirements under section 402(3)(A) of the Maine Freedom of Access Act (1 MRSA § 402(3)(A));
- B. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010;
- C. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under the Maine Criminal History Record Information Act (16 MRSA c. 3, sub-c. 8). However, certain law enforcement records must be made available for inspection and copying to the extent permitted under that Act;
- D. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist

attack is exempted from disclosure requirements under the Maine Criminal History Record Information Act (16 MRSA c. 3, sub-c. 8);

- E. Federal, State, Local, or Tribal records that are protected by law.
16. Except as permitted under applicable law,⁹ the existence, content, and source of the information shall not be made available to an individual if there is a reasonable possibility that release or inspection of the information would:
- A. Interfere with law enforcement proceedings (16 MRSA § 614 (1)(A));
 - B. Result in public dissemination of prejudicial information concerning an accused person or concerning the prosecution's evidence that shall interfere with the ability of a court to impanel an impartial jury (16 MRSA § 614 (1)(B));
 - C. Constitute an unwarranted invasion of personal privacy (16 MRSA § 614 (1)(C));
 - D. Disclose the identity of a confidential source (16 MRSA § 614 (1)(D));
 - E. Disclose confidential information furnished only by the confidential source (16 MRSA § 614 (1)(E));
 - F. Disclose trade secrets or other confidential commercial or financial information designated as such by the owner or source of the information or by the Department of the Attorney General (16 MRSA § 614 (1)(F));
 - G. Disclose investigative techniques and procedures or security plans and procedures not generally known by the general public (16 MRSA § 614 (1)(G));
 - H. Endanger the life or physical safety of any individual, including law enforcement personnel (16 MRSA § 614 (1)(H));
 - I. Disclose conduct or statements made or documents submitted by any person in the course of any mediation or arbitration conducted under the auspices of the Department of the Attorney General (16 MRSA § 614 (1)(I));
 - J. Disclose information designated confidential by some other statute (16 MRSA § 614 (1)(J)); or
 - K. Identify the source of complaints made to the Department of the Attorney General involving violations of consumer or antitrust laws (16 MRSA § 614 (1)(K)).
17. If an individual has objections to the accuracy or completeness of the information retained about him or her that has been publicly disclosed, the individual shall submit the objection to the MIAC Director at the following e-mail address: intel.msp@maine.gov. The MIAC Director shall in turn forward the complaint to the MIAC Privacy Officer and the Maine State Police Staff Attorney. The MIAC Privacy Officer shall notify the person filing the objection that the objection has been received within thirty (30) business days. The individual shall be given reasons if requests for correction are denied. The individual shall also be informed that if he or she wishes to appeal the determination of the MIAC to deny his or her request to change the information at issue, the individual may submit a written request to the Colonel of the Maine State Police asking that the Colonel review and reconsider that matter. The Colonel shall do so and render a decision regarding the matter within forty-five (45) business days.
- A. Each such request for correction, and the disposition thereof, shall be manually or electronically documented.

⁹ See 16 MRSA § 614.

Prohibited uses of information

18. Information gathered or collected and records retained by the MIAC SHALL NOT BE:
 - A. Sold, published, exchanged, or disclosed for commercial purposes;
 - B. Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the MIAC; or
 - C. Disseminated to persons not authorized to access or use the information.

Part IX. Information Retention & Destruction

Review of Information Regarding Retention

1. Criminal intelligence information maintained by the center in the MIS shall be reviewed for purging every five (5) years from the date it was received by the MIAC. All applicable tips and SAR information is to be reviewed for purging at least annually from the date the information was received by the MIAC. If the information is found to be unsubstantiated, it is to be immediately purged.
2. All other information maintained by the MIAC shall be reviewed and purged in a time appropriate for the data under the MIAC retention schedule, but no greater than 5 years.
3. When information has no further value or meets the criteria for removal under the center's retention and destruction policy, it shall be purged, destroyed, or deleted. Information shall not be returned to the submitting source.

Destruction of Information

4. The MIAC shall delete intelligence information, unless it is updated, every five (5) years from the date it was obtained, and be compliant with the Federal code of regulations, 28 CFR Pt. 23.
5. If practicable, a record of information to be purged may be reviewed by the MIAC, in appropriate system(s), within 30 days of the required purge date.
6. Notification to or approval by source agencies of proposed destruction or return of records is not required. Agencies that have maintained their own copies of information submitted to the MIAC are solely responsible for auditing and purging/destroying such records in accordance with applicable law and this policy.
7. No record of the purged information shall be maintained by the MIAC, to satisfy the integrity and completeness of the purged information from appropriate systems, with the exceptions of information stated in this policy.

Destruction of Classified National Security Information

8. Classified information ("Secret" and above) maintained by the MIAC shall be audited on an annual basis. This audit shall:

-
- A. Determine if there is a continuous use/need for each classified document stored in the security container;
 - B. Ensure that ALL classified materials being retained have the appropriate classified cover sheets attached;
 - C. Ensure that ALL classified materials being retained are properly marked;
 - D. Ensure that ALL Secret and Top Secret materials are recorded on Classified Material Control Inventory Form CD-481;
 - E. Ensure that ALL Secret/Top Secret materials selected for destruction are recorded on the form CD-481 and are destroyed by approved methods.

Part X. Accountability & Enforcement

Information System Transparency

1. The MIAC shall be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be provided to the public for review, made available upon request, and posted on the center's Web site at www.maine.gov/miac/.