



NEW JERSEY STATE POLICE  
REGIONAL OPERATIONS AND INTELLIGENCE  
CENTER SECTION  
PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES  
POLICY  
2026

## **Table of Contents**

|                                                 |    |
|-------------------------------------------------|----|
| A. Statement of Purpose.....                    | 3  |
| B. Policy Applicability & Legal Compliance..... | 3  |
| C. Governance & Oversight.....                  | 5  |
| D. Definitions.....                             | 7  |
| E. Information.....                             | 7  |
| F. Acquiring and Receiving Information .....    | 12 |
| G. Data Quality Assurance.....                  | 13 |
| H. Collation & Analysis.....                    | 14 |
| I. Merging Records.....                         | 15 |
| J. Sharing & Disclosure.....                    | 16 |
| K. Redress.....                                 | 18 |
| L. Security Safeguards.....                     | 20 |
| M. Information Retention & Destruction.....     | 22 |

N. Accountability & Enforcement.....24

O. Training.....25

**APPENDICES**

Appendix A – Terms and Definitions.....28

Appendix B - Fair Information Practice Principles (FIPPs).....44

Regional Operations & Intelligence Center  
Privacy, Civil Rights, and Civil Liberties Policy

**A. Purpose Statement**

The mission of the Regional Operations & Intelligence Center (“ROIC” or “Center”) is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the State of New Jersey while protecting privacy, civil rights, civil liberties (P/CRCL), and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected.

The purpose of this P/CRCL protection policy is to promote the ROIC and user conduct that complies with applicable federal, state, local, tribal, and territorial law and assists the Center and its users in:

- increasing public safety and improving national security.
- minimizing the threat and risk of injury to specific individuals.
- minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
- minimizing the threat and risk of damage to real or personal property.
- protecting individual P/CRCL, and other protected interests.

- protecting the integrity of the criminal investigation, criminal intelligence, and justice system processes and information.
- minimizing the reluctance of individuals or groups to use or cooperate with the justice system.
- supporting the role of the justice system in society.
- promoting governmental legitimacy and accountability.
- not unduly burdening the ongoing business of the justice system.
- making the most effective use of public resources allocated to public safety agencies.

Refer to *Appendix A – Terms and Definitions* for a list of key terms and definitions.

## **B. Policy Applicability and Legal Compliance**

1. All ROIC personnel, participating agency personnel, personnel providing information technology services to the Center, staff members in other public agencies, private contractors providing services to the Center, and other authorized users who are not employed by the Center or a contractor will comply with the Center's P/CRCL policy. This policy applies to information the Center gathers, collects, or receives, as well as information it 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. The ROIC will provide a printed or electronic copy of this policy to all Center personnel, non-Center personnel who provide services to the Center, and to participating agencies and individual users. The ROIC will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains. For information on non-compliance, refer to Section N.3.a.
3. The ROIC requires all personnel, participating agency personnel, personnel providing information technology services to the Center, private contractors, agencies from which Center information originates, and other authorized users to comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to Federal, State, and Local Laws, Regulations, and Guidance Relevant.



4. The ROIC has adopted internal operating policies that comply with applicable laws protecting P/CRCL, including, but not limited to those set forth in all Federal, State, and Local Laws, Regulations, and Guidance Relevant to Seeking, Retaining, and Disseminating Justice Information.

- U.S. Constitution.
- U.S. Constitution, Amendments I-XXVII.
- U.S. Congress. National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495. July 26, 1947, as amended.
- U.S. President. Executive Order 12333, United States Intelligence Activities. December 4, 1981.
- U.S. President. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 25, 2005.
- Office of the Director of National Intelligence. Privacy Guidelines for Sharing Protected Information. 2009.
- Office of the Director of National Intelligence. Intelligence Community Policy Guidance No. 101.1. 2009.
- Office of the Director of National Intelligence. Intelligence Community Directive 107: Civil Liberties, Privacy and Transparency. 2018.
- U.S. Department of Justice, Criminal Intelligence Systems Operating Policies, 28 CFR Part 23. 1998.
- U.S. President. Executive Order 12958, Classified National Security Information. April 17, 1995.
- State of New Jersey. Executive Order No. 5. March 16, 2006..
- New Jersey Office of the Attorney General. Attorney General Guidelines on Collection, Handling, Storage and Dissemination of Intelligence in New Jersey. 2004.
- State of New Jersey. New Jersey Domestic Security Preparedness Act. P.L. 2001, c. 246.
- State of New Jersey. Open Public Records Act, N.J.S.A. 47:1A-1 et seq. (P.L. 2001, c. 404), as amended.
- State of New Jersey. New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 et seq. (P.L. 2005, c. 226).
- State of New Jersey. Law Against Discrimination, N.J.S.A. 10:5-1 et seq.
- New Jersey, Strengthening Trust Between Law Enforcement and Immigrant Communities. P.L. 2026, c. 5 A4071/S3521 (“Immigrant Trust Act”).
- New Jersey, Privacy Protection Act. P.L. 2026, c. 4 A4070/S3522.
- U.S. Department of Justice, Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Security Policy. 2026.

5. All ROIC personnel, participating agency personnel, personnel providing information technology services to the Center, private contractors, agencies from which the Center information originates, and other authorized users will comply with applicable laws protecting P/CRCL.

6. The ROIC has adopted internal operating policies in compliance with applicable laws protecting P/CRCL.

### **C. Governance and Oversight**

1. Primary responsibility for the operation of the ROIC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the development, modification, and enforcement of this policy is assigned to the Commanding Officer (CO) of the ROIC Section.

2. The ROIC is guided by the Privacy and Civil Liberties Oversight Committee (Committee) that works to ensure that P/CRCL are protected as provided in this policy and by the Center's information-gathering and collection, retention, and dissemination processes and procedures. The Committee will consist of the bureau chiefs of the ROIC's Critical Infrastructure Bureau, the Information and Intelligence Analysis Bureau, and the Watch and Warning Bureau. The following optional Committee members may also be included at the discretion of the CO:

- other ROIC personnel designated by the CO.
- New Jersey State Police (NJSP) personnel who the CO may request to serve on the Committee.
- an independent criminal justice expert designated by the CO to provide impartial review, guidance, or evaluation related to criminal intelligence activities.

The Committee will annually review and identify recommended updates to the P/CRCL policy to the Privacy and Civil Liberties Officer (PCLO), in response to changes in law and implementation experience, including the results of audits and inspections, and will solicit input from stakeholders on the development of or proposed updates to the policy.

3. The Committee is guided by a trained PCLO who is appointed by the CO of the Center. The PCLO will serve as the chair of the Committee and will be responsible for:

- reviewing and assessing the recommendations submitted by the Committee for clarity, completeness, and compliance with established standards; raising questions and requesting clarification or revisions, as needed; and submitting the final reports and recommendations pertaining to audits and P/CRCL policy changes to the CO.
- receiving reports regarding alleged errors and violations of the provisions of this policy.
- receiving and coordinating complaint resolution under the Center's redress policy.
- serving as the liaison for the Center (and for the ISE), ensuring that P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

The PCLO can be contacted at the following address: ROIC c/o New Jersey State Police, 2 Schwarzkopf Drive, West Trenton, NJ 08628 and at [ROICPrivacyOfficer@njsp.gov](mailto:ROICPrivacyOfficer@njsp.gov).

4. The ROIC's PCLO ensures that enforcement procedures and sanctions are adequate and enforced. See Section N.3, Enforcement.

**D. Definitions (See *Appendix A-Terms and Definitions*)**

**E. Information**

1. The ROIC will seek or retain information (including "protected attributes") subject to conditions articulated in Section E.2., that:

- is based on a possible threat to public safety or the enforcement of criminal law, or
- is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
- is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
- the source of the information is reliable and verifiable or limitations on the quality of the information are identified, and

- the information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

The ROIC may retain protected information that is based on a level of suspicion that is less than “reasonable suspicion,” such as tips and leads subject to the policies and procedures specified in this policy.

2. Civil Rights and First Amendment Safeguards in Center Operations and Information Sharing.

a. Collection and Retention.

i. General Rule: In accordance with applicable laws, guidance, and regulations, the ROIC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.

ii. **Special Rules for the Collection of Covered Personal Information.** The Center shall not request or collect Covered Personal Information<sup>1</sup> (immigration status, citizenship status, place of birth, social security number, or individual taxpayer identification number) from an individual or a nongovernmental entity except when the collection is necessary to assess eligibility for, or to provide or administer, a public service, benefit, program, or professional qualification or license, or as otherwise required by State law.

iii. Source Notification Obligations. The Center will inform information-originating agencies not to submit information to it that is subject to the safeguards in Section E(2)(a).

b. Prohibition on Discriminatory Use.

i. Center personnel shall not consider an individual's race or ethnicity as a factor in drawing an inference or conclusion that the person may be involved in criminal activity or as a factor in exercising police discretion as to how to stop or otherwise

---

<sup>1</sup> See Appendix A, Terms and Definitions.



treat the person, subject to the exceptions set forth in Subsection E(2)(b)(ii) of this policy. This restriction applies to intelligence and information-sharing activities, including:

- Participation in any stage of the intelligence cycle in which race or ethnicity is used as a factor in drawing an inference or conclusion about an individual's involvement in criminal activity or in making any determination in exercising police discretion as to how to stop or otherwise treat an individual;
- Provision of assistance to federal immigration authorities when the sole purpose is to enforce federal civil immigration law, including:<sup>2</sup>
  - Participating in, providing analytical support for, or contributing information to civil immigration enforcement operations;
  - Disclosing non-public personally identifying information (PII) to federal immigration authorities;<sup>3</sup> and
  - Providing access to any State, county, or municipal law enforcement equipment, office space, database, or property not available to the general public.
- Provision of notice of a detained individual's upcoming release from custody, unless the detainee meets the criminal history thresholds<sup>4</sup> or is subject to a Final Order of Removal signed by a federal judge under applicable law and such final order is lodged with the county jail or State prison where the detainee is being held;
- Use of Center resources, personnel, databases, and analytical products to support any operation conducted under a formal agreement in which a State, county, or municipal law enforcement agency has accepted delegated authority to enforce federal civil immigration law;<sup>5</sup> and

---

<sup>2</sup> These activities are prohibited **only when the sole purpose of the request or operation is the enforcement of federal civil immigration law**. Where a federal request or joint operation has a primary law enforcement purpose unrelated to civil immigration enforcement, the restrictions in Section E(2)(b)(i) do not apply, and personnel should document the non-immigration primary purpose in the relevant activity log or product record. When the purpose of a request is ambiguous, personnel shall treat it as civil immigration enforcement for purposes of these restrictions until clarified.

<sup>3</sup> Refer to Appendix A, Terms and Definitions for the definition of this term.

<sup>4</sup> Refer to the Immigrant Trust Act, § 3(c)(5)(a) for the enumerated offenses.

<sup>5</sup> This prohibition applies regardless of whether the agreement was entered into before or after the effective date of applicable State law, and regardless of whether the Center itself is a party to any such agreement.



- Inquiring into an individual's immigration status, unless it is necessary for an ongoing investigation of an indictable offense by that individual and relevant to the offense under investigation.

ii. Exceptions: The following activities are not prohibited by the restrictions set forth in Section E(2)(b)(i) of this policy:

- The restrictions on the use of race or ethnicity do not apply when personnel are responding to or processing a suspect-specific or investigation-specific BOLO situation in which race or ethnicity is part of a documented physical description.
- Personnel may participate with federal authorities in a joint law enforcement task force whose primary purpose is unrelated to civil immigration enforcement. Personnel participating in any such task force shall document the primary law enforcement purpose of the task force in the relevant activity or case record.
- Sharing publicly available information or information readily available to the public (in the method the public can obtain it) with federal immigration authorities is permitted.
- Sending to, maintaining, or receiving from federal immigration information regarding the citizenship or immigration status of any individual is permitted.
- When required by exigent circumstances, providing federal immigration authorities with aid or assistance, including access to non-public information, equipment, or resources is permitted.

3. The ROIC applies labels to Center-originated information (or ensures that the originating agency has applied labels) to indicate to the authorized user that:

- the information is protected information (as defined by the ISE Privacy Guidelines) and, to the extent expressly provided in this policy, includes organizational entities.
- the information is subject to laws restricting access, use, or disclosure.

4. The ROIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:

- whether the information consists of tips and leads, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- the nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- the reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- the validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the ROIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- protect confidential sources and police undercover techniques and methods.
- not interfere with or compromise pending criminal investigations.
- protect an individual's right of privacy and his or her civil rights and civil liberties.
- provide legally required protections based on the individual's status such 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.

6. The labels assigned to existing information under Section E.5 (above) will be reevaluated whenever:

- new information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
- there is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. ROIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads.

- 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.

- Store the information using the same storage method used for data which rises to the level of reasonable suspicion, and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination for personally identifiable information (PII)).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for one year in order to work an unvalidated tip or lead to determine its credibility and value or assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the Center’s physical, administrative, and technical security measures to ensure the protection and security of tips and leads.
- Tips and leads will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The New Jersey Office of Homeland Security and Preparedness (NJOHSP) has implemented processes for the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (suspicious activity report (SAR) process as referred to as “NJSARs”) 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.

9. The ROIC will 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 will provide notice mechanisms, including but not limited to metadata or data field labels, to enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.



10. The ROIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

- the name of the originating Center, department or agency, component, and subcomponent.
- the name of the Center's justice information system from which the information is disseminated.
- the date the information was collected and, when feasible, the date its accuracy was last verified.
- the title and contact information for the person to whom questions regarding the information should be directed.

11. The ROIC will attach (or ensure that the originating agency has attached) specific labels to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification. The ROIC will keep a record of the source of all information sought and collected by the Center.

12. The ROIC will keep a record of the source of all information sought and collected by the Center.

## **F. Acquiring and Receiving Information**

**1. Information-gathering (acquisition) and access and investigative techniques used by the ROIC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:**

- 28 CFR Part 23 regarding "criminal intelligence information," as applicable.<sup>6</sup>

---

<sup>6</sup> The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy and civil liberties. The regulation applies, as a matter of law, to state, local, tribal, or territorial agencies if they are operating interjurisdictional or multijurisdictional criminal intelligence systems that are supported with Omnibus Crime Control and Safe Streets Act funding. See 28 CFR § 23.3. For participating or member agencies, the intelligence project's operating policies, as set forth in a participation or membership agreement, govern their submission, access, use, retention/destruction, and any third-party dissemination of criminal intelligence information received from the intelligence project. Those centers



- the Fair information Practice Principles (FIPPs) but note that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or Center policy. For further information, refer to Appendix B -- Fair Information Practice Principles.
  - criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP) (Ver. 2).
  - United States Constitutional provisions; New Jersey statutes; New Jersey Attorney General Guidelines; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.
2. **Information-gathering and investigative techniques used by the ROIC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.**
  3. **External agencies that access the ROIC's information or share information with the Center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.**
  4. **The ROIC will contract only with commercial database entities that provide an assurance that their methods for gathering PII comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.**
  5. **The ROIC will not directly or indirectly receive, seek, accept, or retain information from:**
    - an individual who or nongovernmental entity that may receive a fee or benefit for providing the information, except as expressly authorized by law or Center policy.
    - an individual who or information provider that is legally prohibited from obtaining or disclosing the information.

#### G. Data Quality Assurance

1. The ROIC will make reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant

---

that are not subject to 28 CFR Part 23 may voluntarily adopt the protections articulated in 28 CFR Part 23 as a matter of policy.

context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met. Refer to Section I, Merging Records, for further information.

2. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]). The ROIC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient. The labeling of retained information will be reevaluated by the ROIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

3. The ROIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the Center identifies information that is erroneous, misleading, obsolete, or otherwise 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 (except when the Center's information source did not act as the agent of the Center in gathering the information).

4. Originating agencies external to the ROIC are responsible for reviewing the quality and accuracy of the data provided to the Center. The Center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

5. The ROIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the Center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

## **H. Collation and Analysis**

1. Information acquired or received by the ROIC or accessed from other sources will be analyzed only by qualified and properly trained individuals who have successfully completed a background check, and have been selected, approved, trained accordingly, and if applicable, possess the appropriate security clearance.
2. Information subject to collation and analysis is information as defined and identified in Section E, Information.
3. Information acquired or received by the ROIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
  - further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the Center.
  - 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 (including terrorist) activities.
4. The ROIC requires that analytical products be reviewed by the PCLO or the relevant Unit Head to ensure alignment with applicable P/CRCL protections prior to dissemination or sharing by the ROIC. To promote consistency across the ROIC, the PCLO will provide cross-unit guidance on P/CRCL safeguards and delivers, or facilitates, annual training on the product-review process. Unit Heads remain responsible for the lawful operation of their units and serve as the final reviewers of all product-related determinations.

## **I. Merging Records**

1. Information will be merged only by qualified individuals who have successfully completed a background check and possess the appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
2. The set of identifiers sufficient to allow merging from records about an individual or organization from two or more sources will consist of all available attributes that can contribute to a higher accuracy of match. The set of identifying information sufficient to allow merging by the

ROIC may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

3. If the matching requirements are not fully met but there is reason to believe the records are about the same individual, or organization, the information may be associated by the ROIC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

## **J. Sharing and Disclosure**

1. Credentialed, role-based access criteria will be used by the ROIC, as appropriate, to control:

- the information to which a particular group or class of users can have access based on the group or class.
- the information a class of users can add, change, delete, or print.
- to whom, individually, the information can be disclosed and under what circumstances.

2. Access to or disclosure of records retained by the ROIC will be provided only to persons within the Center or in other governmental agencies who are **authorized** to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the Center and the nature of the information accessed will be kept by the Center.

3. Agencies external to the ROIC may not disseminate information accessed or disseminated from the Center without approval from the Center or other originator of the information.



4. Records retained by the ROIC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the Center and the nature of the information accessed will be kept by the Center.

5. Information gathered or collected, and records retained by the ROIC may be accessed or disseminated for *specific purposes* upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the Center and the nature of the information accessed will be kept for a minimum of 5 years by the Center.

6. Information gathered or collected, and records retained by the ROIC may be accessed or disclosed to a member of the public only if the information is defined by law [N.J.S.A. 47:1A-1] to be a public record or otherwise appropriate for release to further the Center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the Center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the Center and the nature of the information accessed will be maintained.

7. Information gathered or collected and records retained by the ROIC will not be sold, published, exchanged, or disclosed for commercial purposes; 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 agency or specifically authorized by the originating agency; or disseminated to persons not authorized to access or use the information.

8. Several categories of records are not ordinarily provided to the public, including:

- records required to be kept confidential by law are exempted from disclosure requirements under N.J.S.A. 47:1A-1 et seq., as amended.
- information determined by the federal government to meet the definition of "classified information" as defined in the National Security Act, 50 U.S.C. § 3001, et seq., and in

accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

- investigatory records of law enforcement agencies that are exempted from disclosure requirements under N.J.S.A. 47:1A-1 et seq.. However, certain law enforcement records must be made available for inspection and copying.
- 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 Open Public Records Act, N.J.S.A. 47:1A-3, Executive Order #26 (McGreevey 2002), Executive Order #9 (Hughes 1963). The Government Records Council also found that criminal intelligence information is confidential under federal regulations and is, therefore, not accessible under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1, et seq. OPRA. Durkin v. New Jersey State Police, Denial of Access Compl. No. 2002-30 (Feb. 13, 20023 Final Decision). By way of example, this may include a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- protected federal, state, local, tribal, or territorial records, which may include records originated and controlled by another agency that cannot, under N.J.S.A. 47:1A-3, Executive Order #26 (McGreevey 2002), Executive Order #9 (Hughes 1963), and the New Jersey Attorney General's guidelines, be shared without permission.
- a record, or part of a record that constitutes trade secrets or information that is commercial, financial, or otherwise subject to a nondisclosure agreement that was obtained from a person, is privileged, and confidential. N.J.S.A. 47:1A-1.1.A

9. Notice of Compelled Disclosure: When the Center is compelled by valid judicial order, judicial warrant, or federal law to disclose Covered Personal Information about an individual, the CO or PCLO Officer will immediately notify the New Jersey Office of the Attorney General. The Office of the Attorney General will notify the person to whom the record pertains within 90 days of disclosure, except where the notice would compromise a criminal investigation. Consistent with New Jersey law, the notice will identify:

- the specific record disclosed.
- the party to whom it was disclosed.
- the basis for the disclosure.

10. The ROIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

## **K. Redress**

### **K.1 Disclosure**

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 2., below, 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 ROIC. 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 will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual by the ROIC's PCLO for not less than three (3) years.

2. The existence, content, and source of the information will not be made available by the ROIC to an individual when:

- disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution [N.J.S.A. 47:1A-3(b)].
- disclosure would endanger the health or safety of an individual, organization, or community [N.J.S.A. 47:1A-3(c)].
- the information is in a criminal intelligence information system subject to 28 CFR Part 23 [Title 28 CFR § 23.20(e)].
- the information source does not reside with the Center.
- the Center did not originate and does not have a right to disclose the information.
- other authorized basis for denial.

If the information does not originate with the Center, the requestor will be referred to the originating agency, if appropriate or required, or the Center will notify the source agency of the request and its determination that disclosure by the Center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

### **K.2 Correction**

1. If an authorized person under Section K1 requests correction of information originating with the ROIC that has been disclosed, the Center's PCLO or designee will inform the individual of the



procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for correction and the resulting action, if any.

### K.3 Appeal

1. If an authorized person to whom information has been disclosed which originated with the ROIC and has requested corrections pursuant to Section K2, the person will be given reasons if requests for correction are denied by the ROIC. The individual will also be informed of the procedure for appeal when the ROIC has cited an exemption for the type of information requested or has declined to correct the challenged information to the satisfaction of the individual to whom the information relates.

### K.4 Complaint

1. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

- a) is exempt from disclosure,
- b) has been or may be shared through the ISE,
- c) is held by the ROIC; and
- d) allegedly has resulted in demonstrable harm to the complainant.

The Center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the ROIC's PCLO at the following address: ROIC c/o New Jersey State Police, 2 Schwarzkopf Drive, West Trenton, NJ 08628. Complaints can be submitted electronically to: [ROICPrivacyOfficer@njsp.gov](mailto:ROICPrivacyOfficer@njsp.gov).

The PCLO will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the Center, the PCLO will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the Center that is the subject of a complaint will be reviewed within thirty



(30) days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within thirty (30) days, the Center will not share the information until such time as the complaint has been resolved. A record will be kept by the Center of all complaints and the resulting action taken in response to the complaint.

2. To delineate protected information shared through the ISE from other data, the ROIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

#### **L. Security Safeguards**

1. The ROIC's PCLO or designee is designated and trained to serve as the Center's security officer.
2. The Center will comply with generally accepted industry or other applicable standards for security. Security safeguards will cover any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related ROIC activity.
3. The ROIC will operate in a secure facility protected from external intrusion. The Center will utilize secure internal and external safeguards against network intrusions. Access to the Center's databases from outside the facility will be allowed only over secure networks.

The ROIC will secure tips and leads information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

4. The ROIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged by personnel unauthorized to take such actions.
5. Access to ROIC information will be granted only to Center personnel whose positions and job duties require such access; who have successfully completed a background check and possess an

appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

6. Queries made to the ROIC's data applications will be logged into the data system identifying the user initiating the query.

7. The ROIC will utilize watch logs to maintain audit trails of requested and disseminated information.

8. To prevent unauthorized public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

9. All individuals subject to this policy who have authorized access to NJSP information assets are responsible for reporting a suspected or actual security or privacy incident no later than one (1) hour after reasonable belief that a security or privacy incident has occurred, consistent with applicable laws, regulations, policies, and procedures. This includes a data breach in any medium or form, including all information, data, devices, hardware, software, services, or other components of information or communications systems. Refer to Appendix A -- *Terms and Definitions* for the definition of "data breach."

a) Suspected information security and privacy incidents may be reported via the following channels:

- Immediate supervisor;
- NJSP IT Service Desk – 609-882-2000 Ext. 2169;
- NJSP Chief Information Security Officer (CISO);
- NJSP Human Resources Representative; or
- New Jersey Cybersecurity Communications and Integration Cell (NJCCIC) Incident Reporting Hotline – 609-963-6900 Ext. 7863 or <https://www.cyber.nj.gov/cyber-incident>

b) Upon notification from a user of a suspected or actual information security or privacy incident, the receiving entity will document the information provided and notify the NJSP CISO and/or ROIC PCLO or their designees of the report; and

c) Beyond the reporting obligations outlined in Section L.9(a) for suspected or actual security or privacy incidents, all individuals will report cyber security incidents to the NJCCIC Incident Reporting Hotline - 609-963-6900 Ext. 7863 or <https://www.cyber.nj.gov/cyber-incident> -- as required by P.L.2023, c.19 (C.52-17B-193.3).

10. Following an assessment of the suspected or confirmed security or privacy incident and as soon as practicable, the ROIC PCLO will notify the originating agency from which the Center received PII of the nature and scope of a suspected or confirmed breach of such information.

The ROIC adheres to N.J.S.A. 56:8-163. The Commanding Officer of the ROIC, in consultation with the NJSP Privacy Officer and the Office of the Attorney General, will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

#### **M. Information Retention and Destruction**

1. The retention and destruction of information and intelligence held by the ROIC is as follows:

- all criminal intelligence information will be reviewed for record retention (validation or purging) by the ROIC at least every five (5) years, in accordance with 28 CFR Part 23<sup>7</sup> and the New Jersey Intelligence System (NJIS) Operating Policy and Procedures.
- unvalidated tips or leads or leads may be retained for up to one year in accordance with Section E.7 (above).

---

<sup>7</sup> Title 28 CFR § 23.3(b)(3) defines “criminal intelligence information” as “data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.” Only those criminal intelligence records that meet the reasonable suspicion criteria and the other 28 CFR Part 23 operating principles and are shared between agencies by an intelligence project are subject to the regulation. Fact-based or uncorroborated information (case investigative files, case management systems, incident/offense reports, field interview cards or contact files, criminal history records, arrest blotters, records management system [RMS] data, tips and leads, suspicious activity reports [SARs], etc.) and other types of information or intelligence gathered/collected and shared by state, local, tribal, or territorial law enforcement and intelligence agencies are not subject to 28 CFR Part 23.

- automated license plate records will be retained in accordance with the New Jersey Attorney General Directive 2022-12, as updated and amended, applicable standard operating procedure, and agreements.
  - information about First Amendment-related events may be retained for up to three (3) years. This is subject to exceptions:
    - Information that is part of an ongoing investigation will be maintained in accordance with the applicable retention schedule established by the ROIC.
    - If a criminal predicate is identified and the information is retained in a criminal intelligence system, then it is subject to retention provisions in 28 CFR Part 23 and the NJIS Operating Policy and Procedures.
  - For other information or intelligence, the record retention will be established by state law or local ordinance, or in accordance with a retention schedule established by the ROIC.
2. When information has no further value or meets the criteria for removal according to the ROIC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted from the database and any backup systems.
3. The ROIC will purge (delete) information once its retention period has expired as provided by the New Jersey Intelligence System Operating Policy and Procedures – Review and Purge Procedures in accordance with 28 CFR Part 23 and this policy.
4. The procedure contained in the New Jersey Intelligence System Operating Policy and Procedures – Review and Purge Procedures in accordance with 28 CFR Part 23 will be followed by the ROIC for notification of appropriate parties, including the originating agency, before information is purged in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
5. Notification of proposed destruction of criminal intelligence information records may or may not be provided to the originating agency by the ROIC, depending on the relevance of the criminal intelligence information and any agreement with the originating agency.
6. A record of the criminal intelligence information to be reviewed for retention will be maintained by the ROIC and, for an appropriate system(s), notice will be given to the submitter at least thirty (30) days prior to the required review and validation/purge date.



## **N. Accountability and Enforcement**

### **N.1. Information System Transparency**

1. The ROIC will be open with the public regarding its information and intelligence collection practices. The Center's P/CRCL policy will be provided to the public for review, made available upon request, and posted on the Center's website -- New Jersey Regional Operations & Intelligence Center (NJ ROIC) | New Jersey State Police.
2. The ROIC's PCLO will be responsible for receiving and responding to inquiries and complaints about P/CRCL protections in the information system(s) maintained or accessed by the Center. The PCLO can be contacted at Regional Operations & Intelligence Center, 2 Schwarzkopf Drive, Ewing, NJ 08628 and reached electronically at ROICPrivacyOfficer@njsp.gov.

### **N.2. Accountability**

1. The audit log of queries made to the ROIC will identify the user initiating the query. The electronic methods and techniques used shall be consistent with the NJSP, Identification and Information Technology Section, Information Technology Bureau.
2. The ROIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for up to five (5) years beyond the applicable retention period for this type of request for access to information for specific purposes and of what information is disseminated to each person in response to the request.
3. The ROIC will adopt and follow procedures and practices to ensure and evaluate the compliance of users with applicable law, system requirements, and the provisions of this policy. The audit trail will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least quarterly, and a record of the audits will be maintained by the PCLO of the Center. Audits will be conducted by designated ROIC representatives. Appropriate elements of this audit process, key audit outcomes, and remedial actions, will be compiled into a report and provided to the CO.

4. The ROIC's personnel or other authorized users shall report errors and suspected or confirmed violations of Center policies relating to protected information to the Center's PCLO.
5. Audits and inspection of the information and intelligence contained in its information system(s) are conducted quarterly and randomly by designated ROIC representatives:
  - i. Quarterly audits may include any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related ROIC activity.
  - ii. Random audits may also be conducted, at the discretion of the designated ROIC representative, without announcement, at any time and without prior notice to staff of the Center.

Audits will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the Center's information and intelligence system(s).

6. The ROIC's Committee guided by the appointed and trained PCLO will review and update the P/CRCL policy annually and will make appropriate changes in response to changes in applicable law, technology, and the purpose and use of the information system.

### 3. ENFORCEMENT

a) If Center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the CO of the ROIC may:

- suspend or discontinue access to information by the Center personnel, the participating agency, or the authorized user.
- apply administrative actions or sanctions as provided by the NJSP rules and regulations or as provided in agency/Center personnel policies.
- if the authorized user is from an agency external to the ROIC, request that the user's employer enforce the policy's provisions.
- refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

b) The ROIC reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center's P/CRCL policy.

## **O. Training**

1. The ROIC will require the following individuals to participate in training programs regarding implementation of and adherence to the P/CRCL policy:

- all Center personnel.
- participating agency personnel.
- personnel providing information technology services to the Center.
- staff members in other public agencies or private contractors providing services to the Center.
- authorized users who are not employed by the Center or a contractor.
- or any other individuals it deems appropriate.

2. The ROIC will provide special training regarding the Center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the ISE.

3. The ROIC's P/CRCL policy training will cover:

- purposes of the P/CRCL protection policy.
- substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the Center.
- State legal requirements, including but not limited to the restrictions of the Immigrant Trust Act and their application to the Center's collection, use, sharing, and disclosure of information, to be completed no later than 60 days after the Division of Criminal Justice training program becomes available.
- originating and participating agency responsibilities and obligations under applicable law and policy.
- how to implement the policy in the day-to-day work of the user, whether a paper or systems user.
- the potential impact of violations of the agency's P/CRCL policy.
- mechanisms for reporting violations of Center P/CRCL protection policies and procedures.
- how to identify, report, and respond to a suspected or confirmed breach of PII.

- the nature and penalties for policy violations, including transfer, dismissal, criminal liability, and immunity, if any.
- updates to the P/CRCL policy, if any, in response to changes in law and implementation experience.





**APPENDIX A**  
**TERMS AND DEFINITIONS**

**Access**—Information access is being able to get to (usually having permission to use) particular information on a computer. Web access means having a connection to the Internet through an access provider or an online service provider.

With regard to the Information Sharing Environment (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.

**Access Control**—The mechanisms for limiting access to certain information based on a user's identity, authorization, and membership in various predefined groups. Access control can be mandatory, discretionary, or role based.

**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 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**—refers to the ROIC and all participating state agencies of the ROIC.

**Analysis (law enforcement)**—The review of information and its comparison to other information to determine the meaning of the data in reference to an investigation or assessment.

**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 logins and logouts. 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.

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

**Authentication**—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of usernames and passwords. See also Biometrics.

**Authorization**—The process of granting a person, a computer process, or a device access to certain information, services, or functionality. Authorization is derived from the identity of the person, the computer process, or the device requesting access, which is verified through authentication. See also Authentication.

**Biometrics**—A general term used alternatively to describe the measurement and analysis of unique physical and/or behavioral characteristics or the automated process as means of verifying a personal identity. See Glossary, Facial Identification Scientific Working Group (FISWG), Version 3.0, October 22, 2022., [Glossary - v3.0 - 2022.10.22.](#)

**Center**—Refers to the ROIC and all participating state agencies of the ROIC.

**Civil Liberties**—refers to 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.<sup>8</sup> They include 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.

**Civil Rights**—The term “civil rights” refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity,

---

<sup>8</sup> Civil Rights and Civil Liberties Protections Guidance, at 4 (August 2008).

gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federally or state protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. The term “civil rights” involves positive (or affirmative) government action to protect against infringement, while the term “civil liberties” involves restrictions on government.<sup>9</sup>

**Collect**—For purposes of this document, “gather” and “collect” mean the same thing.

**Computer Security**—The protection of information technology assets through the use of technology, processes, and training.

**Confidentiality**—Refers to the obligations of individuals and institutions to appropriately use and protect information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies.

**Covered Personal Information** — Information relating to a person's immigration status, citizenship status, place of birth, social security number, or individual taxpayer identification number, as described in sections 4 and 5 of the Privacy Protection Act, P.L. 2026, c. 4. This term is distinct from but included in the scope of "protected information" as used elsewhere in this policy (and defined below) in reference to the ISE and intelligence community frameworks.

**Credentials**—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

**Criminal Activity**—A behavior, an action, or an omission that is punishable by criminal law.

---

<sup>9</sup> The definition of “civil rights” is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6, available at [https://it.ojp.gov/documents/National\\_Criminal\\_Intelligence\\_Sharing\\_Plan.pdf](https://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf), and Civil Rights and Civil Liberties Protections Guidance, at 5.

**Criminal Intelligence Information**—Information deemed relevant to the identification of, and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

**Data**—Inert symbols, signs, descriptions, or measures; elements of information.

**Data Breach**—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personal Identifying Information (PII) or (2) an authorized user accesses or potentially accesses PII for a purpose other than the authorized purpose.

The Center's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted, posting such information on the Internet.
- unauthorized employee access to certain information.
- moving such information to computer otherwise accessible from the Internet without proper information security precautions.
- intentional or unintentional transfer of such information to a system that is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- transfer of such information to the information systems of a possibly hostile agency or an environment where it may be exposed to more intensive decryption techniques.

**Data Protection**—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

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



accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See *Appendix B* for further background on the FIPPs.

**Disclosure**—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or an 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.

**Electronically Maintained**—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

**Electronically Transmitted**—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video conferencing, or messages left on voice mail.

**Evaluation**—An assessment of the reliability of the source and accuracy of the raw data.

**Fair Information Practice Principles (FIPPs)**—FIPPs are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8 below) may be of limited applicability in intelligence operations, as fusion Centers do not generally

engage with individuals. That said, fusion Centers and all other integrated justice systems should endeavor to apply the FIPPs where practicable.

The eight principles are:

1. Purpose Specification
2. Data Quality/Integrity (see definition)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (see definition)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See *Appendix B* for further background on the FIPPs.

**Firewall**—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

**Fusion Center**—Defined in the ISE-SAR Functional Standard, Version 1.5.5 as “[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.” (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion Centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

**General Information or Data**—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management system, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

**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.

**Identification**—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

**Individual Responsibility**—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

**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 three general areas: general data, including investigative information; tips and leads data (including suspicious activity reports); and criminal intelligence information.

**Information Sharing Environment (ISE)**—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

**Intelligence-Led Policing (ILP)**—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multi-source

information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

**Invasion of Privacy**—Intrusion on one’s solitude or into one’s private affairs, public disclosure of confidential information, publicity that puts one in a false light to the public, or appropriation of one’s name or picture for personal or commercial advantage. See also Right to Privacy.

**Judicial warrant**—A warrant based on probable cause and issued by a federal Article III judge or magistrate judge, or the State equivalent. New Jersey, “Strengthening Trust Between Law Enforcement and Immigrant Communities.” P.L. 2026, c. 5 [A4071/S352](#), §2.

**Law**—As used by this policy, law includes the U.S. Constitution, the New Jersey Constitution, and 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.

**Lawful Permanent Resident**—A foreign national who has been granted the privilege of permanently living and working in the United States.



**Least Privilege Administration**—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

**Legitimate Law Enforcement Purpose (aka Valid Law Enforcement Purpose)**—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, public and private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.

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

**Maintenance of Information**—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond its required retention time.

**Metadata**—In its simplest form, metadata is information (data) about information, more specifically, information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

**Need to Know**—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 to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized

government activity, such as to further an investigation or meet another law enforcement requirement.

**Non-public Personally Identifiable Information**— “[I]ncludes a social security number, credit card number, unlisted telephone number, driver’s license number, vehicle license plate number, insurance policy number, and active financial account number and may include the address, telephone number, or email address for an individual’s home, work, or school, if that information is not readily available to the public.” New Jersey, “Strengthening Trust Between Law Enforcement and Immigrant Communities.” P.L. 2026, c. 5 A4071/S352 § 3(c)(2).

**Nonrepudiation**—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

**Non-validated Information**—A tip or lead received by the Center that has been determined to be false, inaccurate, or otherwise determined to not warrant additional action and/or maintenance.

**Originating Agency**—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion Center.

**Participating Agency**—An organizational entity that is authorized to access or receive and use Center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

**Permissions**—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

**Personally Identifiable Information (PII)**—For the purpose of this document, synonymous with personal identifying information, as defined in OAG Directive 2022-12— “Information that can

be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.”<sup>10</sup>

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

**Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy**—A printed, published statement that articulates the policy position of an organization on how it handles the PII that it maintains and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the P/CRCL policy is to articulate that the Center will adhere to those legal requirements and Center policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed and implemented P/CRCL policy uses justice entity resources wisely and effectively; protects the Center, the individual, and the public; and promotes public trust. See *Appendix B* for further information about the FIPPs.

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

**Privacy Protection Act** — P.L. 2026, c. 4 (A4070), Privacy Protection Act.

**Protected Information**—For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to

---

<sup>10</sup> For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, <https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>.

information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion Center or other state, local, tribal, or territorial agency policy or regulation. The term “protected information” includes as a subset of the term “Covered Personal Information.”

For the federal nonintelligence 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 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, policy, or other similar instrument should be covered.

**Public**—Public includes:

- any individual 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 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 Center or participating agency.

Public does not include:

- any employees of the Center or participating entity.
- people or entities, private or governmental, who assist the Center in the operation of the justice information system.
- public agencies whose authority to access information gathered and retained by the Center is specified in law.



**Public Access**—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

**Publicly Available Information**— Publicly available information” means “information that is lawfully made available from federal, State, or local government records or widely distributed media or information that a controller has a reasonable basis to believe a consumer has lawfully made available to the general public and has not restricted to a specific audience.” N.J.S.A. 56:8-166.4 et seq.

**Purge**—A term that is commonly used to describe methods that render data unrecoverable in a storage space or to destroy data in a manner that it cannot be reconstituted. There are different strategies and techniques for data purging, which are often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users.)

**Record**—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

**Redress**—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding *protected information* about them which is under the Center’s control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

**Repudiation**—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

**Retention**—Refer to Storage.

**Right to Information Privacy**—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual’s activities.

**Right to Know**—A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of particular personnel in the course of their official duties.

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

**Security**—Refers to 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 information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

**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:

- 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 retention that do not include computer memory and other in-computer storage. This is the most common meaning in the IT industry.
- 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.

Regarding the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including 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.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of “terrorism information” by P.L. 110-53.

**Terrorism-Related Information**—In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in 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 the 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 may include intelligence information.

**Tips and Leads Information or Data**—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, or criminal history records. 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 fall 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.

**Immigrant Trust Act**—Strengthening Trust Between Law Enforcement and Immigrant Communities. P.L. 2026, c. 5 A4071/S3521.

**Unvalidated information**—A tip or lead (including a SAR) received by the Center that has not yet been reviewed to determine further action or maintenance.

**U.S. Person**—Executive Order 12333 states that a “United States person” means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

**User**—An individual representing a participating agency who is authorized to access or receive and use a Center’s information and intelligence databases and resources for lawful purposes.

**Validated Information**—A tip or lead (including a SAR) that has been reviewed and, when appropriate, combined with other information or further vetted and is determined to warrant additional action, such as investigation or dissemination, and/or maintenance as per the applicable record retention policy.

**Valid Law Enforcement Purpose**—Refer to the definition of legitimate law enforcement purpose.



## **Appendix B**

### **Fair Information Practice Principles<sup>11</sup>**

Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the core elements of the FIPPs can be found:

- At the heart of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.<sup>12</sup>
- Mirrored in many states' laws and in fusion centers' privacy policies.
- In the ISO/IEC 29100 Privacy Framework, which has been adopted by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the ISE by the U.S. Department of Homeland Security (DHS).<sup>13</sup> Note, however, that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy.

- 1. Purpose Specification**—Agencies should specifically articulate the authority that permits the collection of PII. The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

---

<sup>11</sup> Appendix from the Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0.

<sup>12</sup> 5 U.S.C. § 552a.

<sup>13</sup> 6 U.S.C. § 142

*Implementing the Purpose Specification Principle*—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

- ensure that a valid lawful purpose exists and is documented for all collection of PII.
- include the source and authority for the data so that access restrictions can be applied.
- upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially, and limit agency use to only those uses compatible with the original purpose supporting collection.
- ensure that metadata or other tags are associated with the data as it is shared.
- institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitations before permitting use or sharing of data for purposes other than that for which it was collected.

**2. Data Quality/Integrity**—PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

*Implementing the Data Quality/Integrity Principle*—One important way to minimize potential downstream P/CRCL concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Approaches include:

- properly labeling PII.
- determining a policy for safeguarding PII if there are “mixed” databases (i.e., those databases with PII on U.S. individuals and others, regardless of nationality).
- instituting a source verification procedure to ensure reporting is based only on authorized data.
- reconciling and updating PII whenever new relevant information is collected.
- developing a protocol for ensuring data corrections are passed to those entities with which information has been shared.
- creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

**3. Collection Limitation/Data Minimization**—PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

*Implementing the Collection Limitation/Data Minimization Principle*—Collection limitation may be implemented by:

- designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
- limiting data field elements to only those that are relevant.
- ensuring that all distributed reports and products contain only that PII that is relevant and necessary (nothing extraneous or superfluous).
- ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation**—PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

*Implementing the Use Limitation Principle*—Sharing information should be tempered by adherence to key principles such as “authorized access.” Use limitations may be implemented by:

- limiting users of data to those with credential-based access.
- requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
- requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
- prior to sharing information, verify that partners have a lawful purpose for requesting information.
- creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards**—Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

*Implementing the Security/Safeguards Principle*—This principle can be implemented by:

- maintaining up-to-date technology for network security.
- ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.

- ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
- implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
- ensuring that data system purge protocols include complete record deletion on all backup systems.
- Transitioning older repositories into more modern systems to improve access controls.
- masking data so that it is viewable only to authorized users.
- maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- requiring authorized users to sign nondisclosure agreements.

**6. Accountability/Audit**—Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

*Implementing the Accountability/Audit Principle*—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

- ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
- conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII.
- tailoring training to specific job functions, database access, or data source/storage requirements.
- conducting regular audits of all systems in which records are kept ensuring compliance with the P/CRCL policies and all legal requirements.
- following a privacy incident handling procedure for any data breaches or policy violations.
- denying database access to individuals until they have completed mandatory systems access training (including training for handling PII), show a mission need for access, and have any necessary clearances.
- developing targeted and consistent corrective actions whenever noncompliance is found.

**7. Openness/Transparency**—To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination,



and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

*Implementing the Openness/Transparency Principle* -- Agencies can implement the Openness/Transparency principle by:

- providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
- publishing the P/CRCL policy and redress procedures.
- meeting with community groups through initiatives or through other opportunities to explain the agency's mission and P/CRCL protections.
- responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
- conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

**8. Individual Participation**—To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

*Implementing the Individual Participation Principle*—To the extent appropriate, agencies can implement the Individual Participation principle by:

- collecting information directly from the individual to the extent possible and practical.
- providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
- putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.