STACC/SAIC Privacy and Civil Rights/Civil Liberties (P/CRCL) Policy

Policy/Procedure Number:	**OHS-200.03.01**
Date of Creation/Revision:	**4/9/19**
Priority Review:	**STACC/SAIC Personnel and Partners**
Distribution:	**STACC/SAIC; Public**

SUMMARY OF REVISIONS

Re-format of policy – minor content changes to reflect updated federal guidance and recommendations from the Peer-to-Peer review with Pennsylvania's state and regional fusion centers.

PURPOSE

A. The Statewide Terrorism Analysis and Crime Center (hereinafter referred to as the "STACC") and the Strategic Analysis and Information Center (hereinafter referred to as the "SAIC") will facilitate effective information and intelligence sharing to prevent, detect, deter, and mitigate criminal incidents and threatened or actual terrorist events, working with and supporting local, state and federal governmental agencies, public and private sectors, and the citizens of Ohio.

B. The STACC/SAIC has created and will abide by a P/CRCL Policy ("Policy"), contained herein, to ensure that its information sharing and analysis does not violate any individual privacy rights, civil rights, civil liberties (P/CRCL), or other protected interests. This Policy sets forth guidelines and procedures which comply with state and federal privacy laws that STACC/SAIC personnel must follow in their furtherance of the STACC/SAIC's mission.

POLICY/PROCEDURE

A. APPLICABILITY

1. All STACC/SAIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with this Policy concerning the information the center collects, receives, maintains, archives, accesses, or discloses to center personnel, governmental agencies (including Information Sharing Environment [ISE] agencies), and participating criminal justice and public safety agencies, as well as to private contractors and the general public.

2. The STACC/SAIC will provide a printed or electronic copy of this Policy to all agency and non-agency personnel who provide services to the agency and will require a written acknowledgement of receipt of this Policy and agreement to comply with this Policy and the provisions it contains.

3. All STACC/SAIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized

users will comply with the applicable laws of the State of Ohio (including, but not limited to, R.C. §§109.57, 149.43, 149.433, 1347.01-1347.15, 2953.32, 2953.52, 5502.03, 5503.02, 5503.10), the Ohio Constitution (e.g., Article I, §§1, 3, 4, 11) and the U.S. Constitution (e.g., Bill of Rights, 1st, 2nd, 4th, 5th, 14th Amendments). Criminal Intelligence Data shall be kept in accordance with 28 C.F.R. Part 23.

4. The STACC/SAIC has adopted internal operating policies that are in compliance with the aforesaid applicable laws protecting privacy, civil rights, and civil liberties, as well as the Privacy Act of 1974 (5 U.S.C. 552a), the Driver's Privacy Protection Act (18 U.S.C. §2721 et. seq.), federal wiretap laws (18 U.S.C. §2510, et seq.; 47 U.S.C. §605), and federal laws regarding civil rights litigation (42 U.S.C. §1983).

B. DEFINITIONS

ACCESS**:** Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the Internet through an access provider or an online service provider. For data access, access is usually specified as read-only access and read/write access.

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

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

AGENCY/CENTER**:** Agency/Center refers to the STACC/SAIC and all participating local, county, state agencies of the STACC/SAIC.

AUDIT TRAIL**:** A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail - what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) 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 user names and passwords. See Biometrics.

AUTHORIZATION: The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

BIOMETRICS – Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

CIVIL LIBERTIES: Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. Freedoms guaranteed by the Bill of Rights - the first ten Amendments to the U.S. Constitution – which protect individuals from improper government action or interference.

CIVIL RIGHTS: Those rights and privileges of equal protection that governmental agencies must afford to all individuals in the US regardless of race, ethnicity, religion, gender, national origin, 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. Generally, the term “civil rights” involves positive (or affirmative) government action, while “civil liberties” involves restrictions on government.

COMPUTER SECURITY: The protection of information assets through the use of technology, processes, and training.

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

CREDENTIALS: Information that includes identification and proof of identification that is used to gain access to local and network resources. E.g., user names, passwords, smart cards, and certificates.

CRIMINAL INTELLIGENCE INFORMATION/DATA**:** 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 acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information.

DATA: Inert symbols, signs, descriptions, or measures; elements of information.

DATA BREACH**:** The unintentional release of secure information to an untrusted environment.

DATA PROTECTION**:** The range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

DISCLOSURE: The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner - electronic, verbal, or written - to an individual, agency, or organization outside of the agency who collected it. Disclosure is a subset 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 disk optical media, or cloud technology.

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, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail.

FAIR INFORMATION PRACTICE PRINCIPLES (FIPPs): Internationally recognized principles that inform information privacy policies within government and the private sector. These core elements are incorporated into information privacy laws, policies, and governance documents. They provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system, but fusion centers should endeavor to apply the FIPPs where practicable. The 8 FIPPs are:

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

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.

GENERAL INFORMATION OR DATA**:** Information that could include records, documents, or files pertaining to law enforcement operations (e.g., Computer Aided Dispatch (CAD) data, incident data, management information) and is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

HOMELAND SECURITY INFORMATION**:** As defined in Section 891(f)(1) of the Homeland Security Act of 2002 and codified at 6 USC §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 any person, group, or entity associated with or assisting 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 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

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

INFORMATION SHARING ENVIONMENT (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.

INFORMATION SHARING ENVIRONMENT (ISE) SUSPICIOUS ACTIVITY REPORT (SAR) (ISE-SAR): An ISE-SAR is a SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

INVASION OF PRIVACY: Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private 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.

LAW: Any local, state, or federal constitution, 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 OR 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 they are authorized to perform.

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

MAINTENANCE OF INFORMATION: Applies to all forms of information storage, including electronic systems (e.g., databases) and non-electronic storage systems (e.g., filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or maintain information beyond a time when it no longer serves an organization's purpose.

METADATA: Information (data) about a particular content. 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 upon the type of information and context of use.

NEED TO KNOW: Necessity to obtain or receive criminal intelligence information in the performance of an official law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity.

NON-REPUDIATION: A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

PARTICIPATING AGENCY: An organizational entity authorized to access or receive and use center information, intelligence databases and resources for lawful purposes through its authorized individual users.

PARTICIPATING AGENCY PERSONNEL: Individuals who have signed participating agreements with the Ohio Department of Public Safety and have direct access to the STACC/SAIC's storage of databases, electronic documents and other files.

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

PERSONALLY IDENTIFIABLE INFORMATION (PII)**:** One or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (e.g., height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information - fingerprints, DNA, retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN, Automated Integrated Fingerprint Identification System identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems locations, electronic bracelet monitoring information, etc.).

PERSONS**:** Executive Order 12333 defines "United States persons" as a U.S. citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S. except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means U.S. citizens and lawful permanent residents.

PREOPERATIONAL PLANNING: As defined in ISE-SAR Functional Standard 1.5.5, this refers to "activities associated with a known or particular planned criminal operation or with terrorist operations generally."

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

PRIVACY AND CIVIL RIGHTS/CIVIL LIBERTIES (P/CRL) POLICY**:** A P/CRCL policy is a written, published statement that articulates the policy position of an organization on how it handles the PII that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the P/CRCL policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing 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 agency, the individual, and the public; and promotes public trust.

PRIVACY PROTECTION**:** A process of maximizing the protection of P/CRCL when collecting and sharing information in the process of protecting public safety and public health.

PROTECTED INFORMATION**:** For the non-intelligence community, protected information is information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the U.S. Constitution. For state, local, tribal, and territorial governments, it would include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the US 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. 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 or a state local, or tribal

agency expressly determines by Executive Order, international agreement, other similar instrument, or agency policy should be covered.

PUBLIC**:** Public includes:

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

Public does not include:

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

PUBLIC ACCESS**:** Information that can be seen by the public (i.e., information whose availability is not subject to privacy interests or rights).

REASONABLY INDICATIVE: An operational concept for documenting and sharing suspicious activity that takes into account the circumstances in which the observation is made which created in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

RECORD**:** Any item, collection, or grouping of information that includes PII and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

REDRESS**:** Internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

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 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.

RIGHT TO PRIVACY: The right to be let alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

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

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

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.

2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

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

With regard to the ISE, storage or retention refers to the storage and safeguarding of homeland security information, terrorism information, and law enforcement information by both the originator of the information and any recipient of the information.

SUSPICIOUS ACTIVITY: As defined in Version 1.5.5 of the ISE-SAR Functional Standard, it is "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples include: surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber-attacks, testing of security, etc.

SUSPICIOUS ACTIVITY REPORTS (SAR): The official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity. SARs offer a standardized means for feeding information repositories or data analysis tools. Any patterns identified during SAR data analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

TERRORISM INFORMATION: Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials

support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the US, US persons, or US interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

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

TIPS AND LEADS INFORMATION OR DATA: Uncorroborated reports or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), SARs, and/or field interview reports (FIRs). 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, criminal history records, or CAD data.

A tip or lead can come from a variety of sources, including but not limited to the public, field interview reports, and anonymous or confidential sources. It may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without future information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little to no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning. It is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

USER OR AUTHORIZED USER: An individual (including all STACC/SAIC personnel, participating agency personnel, personnel providing information technology services to the STACC/SAIC, private contractors, and other authorized users) representing a participating agency who is authorized by the STACC/SAIC to access or receive and use the center's information and intelligence databases and resources for lawful purposes.

C. POLICY/PROCEDURE

1. Governance and Oversight

    a. Primary responsibility for the operation of the STACC/SAIC, its justice systems, operations, coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the STACC Operations Commander or Designee or the OHS Security Manager or Designee.

b. The STACC/SAIC shall utilize a privacy oversight team that liaises with community privacy advocacy groups to ensure that P/CRCL are protected as provided in this Policy and by the center's implementing processes and procedures. In conjunction with the STACC Operations Commander or Designee or the OHS Security Manager or Designee, the privacy oversight team will annually review the Policy and make recommendations for changes to the OHS Security Manager or Designee in response to changes in applicable law, implementation experience, and the results of audits and inspections. The privacy oversight team is guided by a center-designated, trained privacy officer. The privacy oversight team and the Privacy and Compliance Officer are appointed by the STACC Operations Commander or Designee or the OHS Security Manager or Designee.

c. The Privacy and Compliance Officer will receive reports regarding alleged errors and violations of the provisions of this Policy, receive and coordinate complaint resolution under the center's redress policy, serve as the center's privacy liaison for the Information Sharing Environment, and, in conjunction with the STACC Operations Commander or Designee or the OHS Security Manager or Designee, ensure that privacy protections are implemented, including the ISE privacy Guidelines, through training, business process changes, and system designs that incorporate privacy enhancing technologies.

2. Information

a. The STACC/SAIC will seek or retain information that:

i. Is based upon a criminal predicate or possible threat to public safety; or
ii. Is based upon reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity; or
iii. 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
iv. Is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches); and
v. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
vi. The information was collected in an authorized and lawful manner, with the knowledge and consent of the individual, if appropriate.

b. The STACC/SAIC will also retain information that does not reach the level of reasonable suspicion requirements, listed above, such as tips and leads or suspicious activity reports (SARs). Refer to Section C.2.k for the center's practices and procedures for this type of information.

c. The STACC/SAIC will keep a record of the source of all information it retains.

d. The STACC/SAIC will not seek or retain information about individuals or organizations solely on the basis of the following: religious, political, or social views or activities; participation in a particular non-criminal organization or lawful event; or race, ethnicity, citizenship, national origin, age, disability, gender, gender identity, or sexual orientation.

e. The STACC/SAIC applies labels to all center-owned information to indicate to the accessing authorized user that:

   i. The information pertains to a United States citizen or lawful permanent resident; and,
   ii. The information is subject to R.C. §§149.43, 149.443 and/or 5502.03, and all applicable state and federal laws restricting access, use, or disclosure of information.

f. Information obtained from other agencies will remain in its original format.

g. The STACC/SAIC personnel will, upon receipt of information, assess the information to determine its nature and purpose. Personnel will assign information to categories to indicate the result of the assessment, such as:

   i. Whether the information is general data, tips and leads data, SARs, or criminal intelligence data;
   ii. The nature of the source (for example, anonymous tip, interview, public records, private sector);
   iii. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
   iv. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

h. At the time a decision is made to retain information, it will be labeled pursuant to applicable limitations on access and sensitivity of disclosure in order to:

   i. Protect confidential sources and police undercover techniques and methods;
   ii. Not interfere with or compromise pending criminal investigations;
   iii. Protect an individual's right of privacy and civil rights and civil liberties; and
   iv. Provide legally required protection based on the status of an individual as a child, sexual abuse victim, a resident of a substance abuse treatment program, a resident of a mental health treatment program, or a resident of a domestic abuse shelter.

i. Labels include "Law Enforcement" (Read, Write, and Modify any material) and "Non-

Law Enforcement" (Read, Write, and Modify only non-law enforcement material). The granting of access shall be restricted to the STACC Operations Commander or Designee or the OHS Security Manager or Designee.

j. The classification of existing information will be reevaluated whenever:

   i. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
   ii. There is a change in the use of the information affecting access or disclosure limitations.

k. STACC/SAIC 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 and SAR information. STACC/SAIC personnel will:

   i. Prior to allowing access to or dissemination of the information, attempt to validate or refute the information and assess it for sensitivity and confidence;
   ii. Subject the information to an evaluation process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated after attempts to validate or determine the reliability of the information fail;
   iii. Store the information using the same storage method used for data that rises to the level of reasonable suspicion, but in a file clearly separate from criminal intelligence, and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information;
   iv. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination). Personnel must sign and adhere to the Policy;
   v. 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 when credible information indicates potential imminent danger to life or property.
   vi. Retain information long enough to work a tip or lead or SAR information to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label;
   vii. Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SAR information will be secured in a system that is the same or similar to, but separate from, the system that secures data that rises to the level of reasonable suspicion;
   viii. The STACC/SAIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-

related information and criminal intelligence. All SAR data within the STACC/SAIC will be clearly identified as such and will be stored in a separate database than criminal intelligence, but will have the same securities as that of criminal intelligence.

l. The STACC/SAIC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the ISE. Furthermore, the center will provide notice mechanisms, including but not limited to metadata and labeling of fields, that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

m. The STACC/SAIC requires certain basic descriptive information to be entered and electronically associated with each piece of data (or content) for which there are special laws, rules, or policies regarding accessed, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

   i. The name of the originating center, department or agency, component, and subcomponent;
   ii. The date the information was collected and the date its accuracy was last verified;
   iii. The title and contact information for the person to whom questions regarding the information should be directed.

n. The STACC/SAIC will apply specific labels and descriptive metadata to information that will be accessed and disseminated to clearly indicate all legal restrictions on information sharing based on information sensitivity or classification. Metadata fields will include: the legal authority, classified information categories, indicator of special clearance required, special access processes, caveats, polygraphs, non-disclosure agreements, and sensitive but unclassified labels.

o. The STACC/SAIC will keep a record of the source of all information it retains.

3. Acquiring and Receiving Information

a. Information gathering and investigative techniques used by the STACC/SAIC and affiliated agencies will comply and adhere to the following regulations and guidelines:

   i. 28 CFR Part 23 with regard to criminal intelligence and the requirement for reasonable suspicion of criminal activity;
   ii. The 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);
   iii. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP) (Ver. 2);

iv. The center will make every reasonable effort to insure that it complies with R.C. Chapter 1347 (Duties of state and local agencies maintaining personal information systems), as well as the U.S. and Ohio constitutions and any other laws or regulations that apply to P/CRCL protections for multi-jurisdictional intelligence and information databases.

b. The STACC/SAIC's SAR and tips and leads process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers, STACC/SAIC staff, participating agencies, and participating personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity associated with terrorism.

c. The STACC/SAIC will identify SAR information related to terrorism that is eligible for sharing in the ISE using the two-step process set forth in the ISE-SAR Functional Standard. Participating personnel will be responsible for vetting and updating information posted to the ISE-SAR shared space by the center.

d. The STACC/SAIC's tips and leads and SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

e. Information gathering and investigative techniques used by the STACC/SAIC will, and those used by originating agencies should, be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

f. Agencies that participate in the STACC/SAIC and provide information to the center are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state law.

g. The STACC/SAIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws and which is not based on misleading information collection practices.

h. The STACC/SAIC will not directly or indirectly receive, seek, accept, or retain information from:
   i. An individual or information provider who has obtained information illegally; or
   ii. An individual or information provider that is legally prohibited from obtaining or disclosing the information.

4. Information Quality Assurance

   a. The STACC/SAIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [See Section C. 6.] has been met.

   b. The STACC/SAIC will put in place a process for additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. The STACC/SAIC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

   c. At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

   d. The STACC/SAIC 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.

   e. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

   f. The STACC/SAIC will conduct periodic data quality reviews of information it originates for dissemination and make every reasonable effort to ensure that information will be corrected or deleted from the system when the center learns that the information 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).

   g. Center participating agencies are responsible for the quality and accuracy of the data provided to the center. Center participating agencies providing data remain the owners of the data contributed. The STACC/SAIC will review the quality of the information it has received from such agencies and advise the appropriate contact person, in writing (including electronically), if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

   h. The STACC/SAIC will use written or documented electronic notification to inform recipient agencies when information previously provided to such agencies by the STACC/SAIC is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, unverifiable, or lacks adequate context such that the rights of the individual may be affected.

5. Collation and Analysis

    a. Information acquired or received by the STACC/SAIC or accessed from other sources under Section C.2. will be analyzed only by qualified individuals who have successfully completed a background check and possess the appropriate security clearance, and have been selected, approved, and trained accordingly.

    b. Information 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; and to provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

6. Merging Information from Multiple Sources

    a. 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.

    b. Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to clearly establish that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can be compared to ensure a high degree of certainty about the match.

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

7. Sharing and Disclosure

    a. Credentialed, role-based access criteria (See Section C.2.h) will be used, as appropriate, to control:

        i. What information a class of users can have access to;
        ii. What information a class of users can add, change, delete, or print; and
        iii. To whom the information can be disclosed and under what circumstances.

    b. The STACC/SAIC adheres to the current version of the ISE-SAR Functional Standard for the SAR process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially associated with terrorism.

    c. Access to information retained by the STACC/SAIC will only be provided ***to authorized persons within the STACC/SAIC or in other governmental agencies***

who are engaged in 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 whom the person is working. An audit trail will be kept of access by or dissemination of information to such persons.

d. Participating agencies may not disseminate STACC/SAIC information without approval from the originator of the information.

e. Information gathered and retained by the STACC/SAIC may be disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those users or purposes specified in the law. An audit trail will be kept for the life cycle of the record, which will include requests for access and information disseminated to each person.

f. Information gathered and retained by the STACC/SAIC may be disclosed ***to a member of the public*** only if the information is defined by law to be a public record or otherwise appropriate for release to further the agency mission and is not excepted from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to the STACC/SAIC for this type of information or when there is a legitimate need. An audit trail will be kept of all requests and of what information is disclosed to a member of the public. See Section C.9. for the STACC/SAIC redress policy.

g. Information gathered and retained by the STACC/SAIC ***will not*** be:

    i. Sold, published, exchanged, or disclosed for commercial purposes;
    ii. Disclosed or published without prior notice to the contributing agency that it is subject to re-disclosure or publication; or
    iii. Disseminated to unauthorized persons.

h. There are several categories of records that will ordinarily ***not be provided*** to the public:

    i. Public records required to be kept confidential by law are exempted from disclosure requirements under R.C. §§149.43, 149.433, and 5502.03.
    ii. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under R.C. §149.43. However, certain law enforcement records must be made available for inspection and copying if not exempted from disclosure.
    iii. 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 R.C. §§149.43, 149.433, and 5502.03, as applicable. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

iv. Protected federal, state, local, or tribal records, which may include records owned or controlled by another agency.
v. Information prohibited from being disclosed pursuant to court order.

i. The STACC/SAIC staff shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

8. Disclosure to the Subject of a Record

a. Upon satisfactory verification (i.e. fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in Section C.8.b. 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 STACC/SAIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information by contacting the Privacy Officer at the following address: Ohio Department of Public Safety, Statewide Terrorism Analysis and Crime Center (STACC), ATTN: Privacy and Compliance Officer, 2855 West Dublin-Granville Road, Columbus, Ohio, 43235. The STACC/SAIC'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.

b. If the exemptions below do not apply, and information exists that was provided from another agency, the STACC/SAIC will refer the request to that agency and assist and facilitate with the communication between the individual and the agency. Either way, the existence, content, and source of the information ***will not*** be made available to an individual when:

i. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (e.g., R.C. §§ 109.57, 149.43, 1347.08, 1347.12, 5502.01, 5502.011, 5502.03, 5503.02);
ii. Disclosure would endanger the health or safety of an individual, organization, or community (e.g., R.C. §§149.433, 1347.12; *Kallstrom v. City of Columbus*, 165 F. Supp. 2d 686, S.D. Ohio, 2001; *State ex rel. Plunderbund Media, L.L.C. v. Born*, 141 Ohio St.3d 422 (2014));
iii. The information is in a criminal intelligence system (28 C.F.R. Part 23);
iv. The information is protected by State or Federal statute (e.g., R.C. §§ 109.57, 149.43, 149.433, 1347.08, 1347.12, 5502.03);
v. The information source does not reside with the STACC/SAIC; or the STACC/SAIC does not own or have a right to disclose the information (i.e., Third-Party Rule).

9. Complaints and Corrections

a. If an individual has complaints or objections to the accuracy or completeness of information retained about him or her ***within a system under the center's control***, and such information is not exempt under Section C.8.b, the STACC/SAIC will inform

the individual of the following procedure for submitting complaints or requesting corrections:

i. Submit a written request to the STACC Privacy and Compliance Officer at the following address: Ohio Department of Public Safety, Statewide Terrorism Analysis and Crime Center (STACC), ATTN: Complaints & Corrections, 2855 West Dublin-Granville Road, Columbus, Ohio, 43235, to investigate the current status of information about the individual.
ii. The STACC/SAIC will, within a reasonable period of time, make a reasonable investigation with the providing agency to determine whether the disputed information is accurate, relevant, timely and complete, and will notify the individual of the results of the investigation.
iii. The STACC/SAIC will correct any identified data/record deficiencies and will purge any information that it cannot verify or otherwise correct.
iv. If the investigation reveals that the information is accurate, relevant, timely and complete, the STACC/SAIC shall include within the system a notation that the individual disputes the information and summarize the individual's position on the disputed information.

b. A record will be kept of all complaints and requests for corrections.

c. If an individual has complaints or objections to the accuracy or completeness of information about him or her that ***originates with another agency within the state***, the STACC Operations Commander or Designee or the OHS Security Manager or Designee will notify the agency that is the owner of the data of the complaint or request for correction and coordinate with the agency to ensure that the individual is provided with complaint submission or corrections procedures. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must either consent to the correction and remove the record, or assert a basis for denial in accordance with R.C. Chapter 1347. This must be done in sufficient time to permit compliance with deadlines found within R.C. Chapter 1347. A record will be kept of all complaints and requests for corrections.

d. If an individual has complaints or objections to the accuracy or completeness of information that has been disclosed to him or her that ***originates from the ISE***, the STACC/SAIC ISE Privacy Officer or designee will notify the ISE agency of the complaint or request for correction and coordinate with them to ensure that the individual is provided with complaint submission or corrections procedures. The owning ISE agency must either correct or remove or assert a basis for denial in a timely manner. A record will be kept of all complaints and requests for corrections.

e. To delineate ISE agency information from other contributing agency data, the STACC/SAIC maintains records of ISE originating agencies the center has access to, as well as audit logs, and employs system mechanisms whereby the source (or owning agency, including ISE agencies) is identified within the information record.

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

10. Security Safeguards

a. The STACC/SAIC's Security Liaison(s) will receive appropriate training and will be designated by the OHS Executive Director or the State Security Point of Contact.

b. The STACC/SAIC will comply with generally accepted industry or other applicable standards for security, which will cover any types of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related STACC/SAIC activity.

c. The STACC/SAIC will operate in a secure facility protecting the facility from external intrusion. The STACC/SAIC will utilize secure internal and external safeguards against network intrusions. Access to STACC/SAIC databases from outside the facility will only be allowed over secure networks.

d. The STACC/SAIC will secure tips, leads and SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

e. The STACC/SAIC will store information in a manner that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as designated by the STACC Operations Commander or Designee or the OHS Security Manager or Designee.

f. Access to center information will only be granted to center personnel whose position and job duties with the center require such access and the individual has successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

g. Queries made to the STACC/SAIC data applications will be logged in the data system and will identify the user initiating the query.

h. The STACC/SAIC will utilize logs to maintain audit trails of requested and disseminated information. Records of dissemination shall be kept with the original data entry.

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

j. If the STACC/SAIC discovers a "breach of the security of the system," as defined in R.C. §1347.12, it shall immediately notify the Privacy and Compliance Officer and

appropriate agency personnel. The STACC/SAIC will notify a resident of this state, about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person which will cause a material risk of identity theft or other fraud to the person, as soon as practical and without unreasonable delay following discovery or notification of the breach. This notification is subject to the legitimate needs of law enforcement to investigate the release and consistent with any measures necessary to determine the scope of the release and reasonably restore the integrity of the data system.

11. Information Retention and Destruction

    a. All criminal intelligence information will be reviewed for record retention (validation or purge) at least every five (5) years, in accordance with 28 C.F.R. Part 23. Additionally, all SAR data will have a retention period of five (5) years, after which point the data will be either validated or purged. All other information will be retained in accordance with agency established record retention schedules.

    b. When information (including printed, handwritten or electronic) has no further value or meets the criteria for removal according to the STACC/SAIC's retention schedules or according to applicable law, it will be purged, destroyed, and deleted, or returned to the submitting source.

    c. The STACC/SAIC will purge, destroy, or delete information or return it to the source, unless it is updated and validated, every five (5) years, which will be compliant with 28 C.F.R. Part 23.

    d. Permission to destroy or return information or records will be presumed if the applicable information is not updated, within the specified time period above.

    e. Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information.

    f. A record of information to be reviewed for retention will be maintained by the STACC/SAIC.

12. Accountability and Enforcement

    a. Information System Transparency

        i. The STACC/SAIC will be open with the public in regard to information and intelligence collection practices. The P/CRCL Policy will be provided to the public for review and made available upon request. This Policy may also be accessed as a resource document off the OHS website at http://homelandsecurity.ohio.gov.
        ii. The STACC/SAIC Privacy and Compliance Officer 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 STACC/SAIC. Inquiries and complaints can be addressed to: Ohio Department of Public Safety, Statewide Terrorism Analysis and Crime Center, ATTN: Privacy and Compliance Officer, 2855 West Dublin-Granville Road, Columbus, Ohio, 43235.

b. Accountability

i. Queries made to the STACC/SAIC data applications will be logged into the data system identifying the user initiating the query.
ii. The STACC/SAIC log will be utilized to maintain an audit trail of requested or disseminated information. An audit trail will be maintained for the life cycle of the applicable record.
iii. The STACC/SAIC will provide a copy of this Policy to all agency and non-agency personnel who provide services and will require written acknowledgement of receipt of this Policy and agreement of compliance to this Policy and the provisions it contains.
iv. The STACC/SAIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this Policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, as to not establish a pattern of the audits. These audits will be mandated at least quarterly and a record of the audit will be maintained by the STACC Operations Commander or Designee or the OHS Security Manager or Designee.
v. The STACC/SAIC's personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information to the center's Privacy and Compliance Officer.
vi. The STACC/SAIC will annually provide for the conduct of an audit and inspection of the information contained in its criminal intelligence system. The audit will be conducted by a designated, independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time, and without prior notice to the STACC/SAIC. This audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system.
vii. The STACC/SAIC's privacy oversight team will annually review and update the provisions protecting P/CRCL contained within this Policy and recommend appropriate changes in response to changes in applicable law, implementation experience, and the results of audits and inspections. (See Section C.1.b).

13. Enforcement

a. If STACC/SAIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, or an authorized user is found to be not complying with the provisions of this Policy regarding the

collection, use, retention, destruction, sharing, classification, or disclosure of information, the STACC Operations Commander or Designee or the OHS Security Manager or Designee will:

i. Suspend or discontinue access to information by the authorized user or user agency;
ii. Suspend, demote, transfer, or terminate the person, as permitted by applicable Ohio Department of Public Safety (DPS) and/or STACC/SAIC policies;
iii. Apply administrative actions or sanctions as provided by DPS rules and regulations or as provided in agency personnel policies;
iv. If the user is from an agency external to the center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
v. Refer the matter to the Ohio State Highway Patrol and/or the Federal Bureau of Investigation for criminal prosecution, as necessary, to effectuate the purposes of the policy.

b. The STACC/SAIC 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 Policy.

14. Training

a. The STACC/SAIC will require the following individuals to participate in training programs regarding the implementation of and adherence to the P/CRCL Policy:

i. All assigned personnel of the center;
ii. Personnel providing information technology services to the STACC/SAIC;
iii. Staff in other public agencies or private contractors providing services to the agency; and
iv. Authorized users who are not employed by the agency or a contractor.

b. The STACC/SAIC will provide special training to personnel authorized to share protected information through the ISE regarding the center's requirements and policies for collection, use, and disclosure of protected information.

c. The STACC/SAIC's P/CRCL Policy training program will cover:

i. Purposes of the Policy;
ii. Substance and intent of the provisions of the Policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the STACC/SAIC;
iii. How to implement the Policy in the day-to-day work of the user, whether a paper or systems user;
iv. The impact of improper activities associated with infraction accessible within or through the agency;

v. Mechanisms for reporting violations of center privacy-protection policies; and the nature and possible penalties for Policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

SPECIAL PROVISIONS

N/A

CURRENT FORM AND SUPPLEMENTAL REFERENCES

N/A

POLICY REFERENCES

N/A

ATTACHMENTS

N/A