

# Privacy Policy

2016

## Vermont Intelligence Center



Kevin Lane

Vermont Intelligence Center

7/15/2016

# Vermont Intelligence Center

## Internal Operations Privacy Policy

### TABLE OF CONTENTS

Topic	Page
1.0 Statement of Purpose	2
2.0 Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties	2
3.0 Definitions	3
4.0 Seeking and Retaining Information	6
5.0 Information Quality	10
6.0 Collation and Analysis of Information	12
7.0 Sharing and Disclosure of Information	12
8.0 Information Retention and Destruction	15
9.0 Accountability and Enforcement	16
10.0 Training	20



## 1.0 Statement of Purpose

The mission of the Vermont Intelligence Center is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal activity, officer safety, and the safety of the public, while following the Fair Information Practices to ensure the rights and privacy of citizens. This policy is to promote the Vermont Intelligence Center and its users' compliance with federal, state, local, and tribal laws and assists 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 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 privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of the criminal investigator, criminal intelligence, and justice system processes and information.
- Minimizing 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.
- Making the most effective use of public resources allocated to public safety agencies.

## 2.0 Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

2.10 All Vermont Intelligence Center (VIC) personnel, participating agency personnel, personnel providing information technology services, private contractors, and other authorized users will comply with the VIC privacy policy. The policy applies to information the VIC collects, receives, maintains, archives, accesses, or discloses to VIC personnel, governmental agencies (including Information Sharing Environment [ISE] participating agencies), and participating justice and public safety agencies, as well as to private contractors and the general public.

2.20 The VIC will maintain an electronic copy of each user's signed privacy policy. Products from the VIC that include Protected Personal Identifiable Information (PII) will include a disclaimer stating the information is not to be disseminated further without the permission of the VIC.

2.30 Requested reports/products with general law enforcement data will include a disclaimer indicating that the data obtained from other agencies is the property of the contributing agencies. Prior approval from the originating agency must be obtained before any specific information about the involvement may be released.

2.40 The VIC will follow the rules established in the Vermont Incident Based Reporting System (VIBRS) User Agreement, maintained by VT Department of Public Safety-Criminal Justice Service.

2.50 VIC personnel and participating agency personnel, personnel providing information technology services, private contractors, and other authorized users shall adhere to all rights granted by the U.S. and Vermont Constitutions.

(a) Provisions of the United States Constitution, and statutory civil rights protections may also directly govern state action. These provisions include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of

Institutionalized Persons Act.

(b) Federal laws, Executive Orders, Regulations, and Policies including CFR Parts 20, 22, and 23 and the Health Insurance Portability and Accountability Act (HIPAA) may affect the sharing of information, including terrorism-related information, in the Information Sharing Environment (ISE).

(c) In addition to the Vermont Constitution, the VIC and its personnel will also adhere to Title 1, Chapter 5, Subchapter 3 of the Vermont Statutes, regarding dissemination of records and Title 9, Chapter 62, Subchapter 63 regarding social security protections.

2.60 The VIC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties including, but not limited to, those listed in section 2.50 of this policy.

### 3.0 Definitions

3.10 Access –Data access is the ability to obtain (through permission from owner) particular information on a computer. Web access means having a connection to the World Wide Web through an access provider or through an online service provider. Data access is usually specified as read-only and/or read/write access.

3.11 Access (with regard to the ISE) – In the context of the ISE, “access” refers to the business rules, means, and processes by and through which ISE participants obtain crime-related information, to include homeland security information, terrorism information, and law enforcement information acquired by another ISE participant.

3.12 Acquisition –The means by which an ISE participant obtains information through the exercise of its authorities. For the purpose of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or information shared with them by another ISE participant who originally acquired the information.

3.13 Agency – The Vermont Department of Public Safety – Vermont State Police.

3.14 Authorized Organizations, Persons, and Users

(a) Authorized Organizations

(i) Law Enforcement Agencies -Federal, State, Local, and Tribal

(ii) Entities, private or governmental, who assist law enforcement agencies in the operation of the justice information system

(iii) Public agencies whose authority to access information gathered and retained by the VIC is specified in law.

(b) Authorized Persons – For the purposes of disclosing and sharing information, persons who are employees or agents of an Authorized Organization who have shown a need to know and a right to know.

(c) Authorized User – An Authorized Person who has been trained and has direct access to one or all of the systems maintained by the VIC. The user also has provided documentation appropriate to the needs of section 9.20. Authorized users outside of the VIC are primarily limited to those who have access to the

Criminal Intelligence Database only.

3.15 Center – All participating agencies within the Vermont Intelligence Center (VIC). The VIC was formerly known as the Vermont Fusion Center (VTFC) under which name this policy was originally approved and adopted. The VIC was subsequently known as the Vermont Information and Analysis Center (VTIAC), which was reflected in a prior revision to this policy.

3.16 Information – 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 the following general areas: general data, tips and leads, suspicious activity reports, criminal intelligence information, and public-open source information.

- (a) General Law Enforcement Information (For purposes of the ISE) or data– Any information obtained by or of interest to a law enforcement agency or official that is both (a) related to crime or the security of 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; assessments of or responses 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.
- (b) 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 report (SIR) information, suspicious activity report (SAR) information, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.
  - i. 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 documents the presence of some suspicion, or is based on a level of suspicion that is less than “reasonable suspicion,” but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.
  - ii. The VIC does participate in a Tips or Leads Data Program. Information within the database will be subject to collection and retention as defined in sections 4.10 and 4.51. The information may be forwarded to law enforcement agencies if believed to be part of an active criminal investigation, or if the information needs validation prior to submission into a criminal intelligence or SAR database. Reports within the Tips and Lead Data Program as subject to purging as defined in 8.10.
- (c) Suspicious Activity Report (SAR) Information – The observation and documentation of a suspicious activity. At the federal level, there are two types of SAR information: 1) SAR information that pertains to suspicious activities that would lead a reasonable person to believe what the person is

observing is reasonably indicative of preoperational planning related to terrorism or other criminal activity; and 2) Banking Secrecy Act SAR information that pertains to suspicious banking activity and is required to be completed by financial institutions. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, the VIC. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

- (d) Criminal Intelligence Information or Data – Information deemed relevant to the identification of criminal activity and those engaged in such activities, or that is reasonably suspected of involvement in criminal acts. These records are maintained in a criminal intelligence system in accordance with 28 C.F.R. Part 23.
- (e) Public –Open Source information – Information that is available to the public and its access is not restricted by the source. This may include but not limited to news reports, internet medium, and town records.

3.17 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.

3.18 Personal Identifiable Information (PII) – Data from which a human being can be uniquely identified as defined by 9 V.S.A. § 2430(5)(a).

3.19 Protected Information –Information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and/or laws of the United States. While not within the definition established by the ISE Privacy Guidelines, protection may be extended to other individuals and organizations by internal federal or Vermont agency policy or regulation.

3.20 Public – Includes:

- (a) Any person, for-profit or nonprofit entity, organization, or association;
- (b) Any governmental entity for which there is no existing law authorizing access to the agency’s information;
- (c) Media organizations;
- (d) 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.

3.21 Public Record – Any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of public agency business, as defined by 1 V.S.A. § 317. Several public records are exempt from public inspection and copying. Included within this list of public records exceptions are:

- a. (5)(A) Records dealing with the detection and investigation of crime, but only to the extent that the production of such records:

- (i) could reasonably be expected to interfere with enforcement proceedings;
- (ii) would deprive a person of a right to a fair trial or an impartial adjudication;
- (iii) could reasonably be expected to constitute an unwarranted invasion of personal privacy;
- (iv) could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source;
- (v) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecution if such disclosure could reasonably be expected to risk circumvention of the law;
- (vi) could reasonably be expected to endanger the life or physical safety of any individual.

b. (B) Records relating to management and direction of a law enforcement agency; records reflecting the initial arrest of a person, including any ticket, citation, or complaint issued for a traffic violation, as that term is defined in 23 V.S.A. § 2302; and records reflecting the charge of a person shall be public.

c. 1 V.S.A. § 317(c)(5)(D): It is the intent of the General Assembly that, consistent with the manner in which courts have interpreted subdivision (A) of this subdivision (5), a public agency shall not reveal information that could be used to facilitate the commission of a crime or the identity of a private individual who is a witness to or victim of a crime, unless withholding the identity or information would conceal government wrongdoing. A record shall not be withheld in its entirety because it contains identities or information that have been redacted pursuant to this subdivision..

d. Critical Infrastructure reports and threat assessments on government and private facilities defined per 1 V.S.A. § 317(c)32.

3.22 Written or Writing – A tangible or electronic record of a communication or representation including handwriting, written or typed printing, photostat, photography, audio or video recording and e-mail.

## **4.0 Seeking and Retaining Information**

4.10 The VIC will seek, retain, or share information that:

- (a) Is based on a criminal predicate or possible threat to public safety; or
- (b) Is based on reasonable predicate that an identifiable individual or organization has committed a criminal offense or is involved in planning criminal conduct or activity that presents a threat to any individual, the community, or any nation and that the information is relevant to the criminal conduct or activity; or
- (c) Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

- (d) Is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches); and
- (e) The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
- (f) The information was collected in a fair and lawful manner.

4.11 The VIC may retain information that is based on a level of suspicion that is less than “reasonable suspicion,” such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures of the originating agency.

4.12 The VIC will not seek or retain information about individuals or organizations solely on the basis of their or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations religious, political, or social views or activities, or their participation in a particular noncriminal organization or event.

4.13 The VIC shall keep record of the source of all information retained by the VIC. The source information shall include the source classification as defined in section 3.0(7) and any caveats from the source on the credibility of the information.

## 4.20 Labeling of Information

- a) The VIC applies labels to center originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
  - i. The information is protected information as defined by the ISE Privacy Guidelines and as defined by the VIC or, to the extent expressly provided in this policy, includes other individuals or organizational entities.
  - ii. The information is subject to local, state or federal law restricting access, use, or disclosure.
- b) The VIC 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:
  - i. Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information.
  - ii. The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
  - iii. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
  - iv. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).
- c) At the time a decision is made by the VIC 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:

- 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 or their civil rights and civil liberties.
  - iv. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.
- d) The labels assigned to existing information under 4.15(c) will be reevaluated whenever:
  - i. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
  - ii. 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.
- e) The VIC 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, thus requiring adherence to existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.
- f) The VIC will attach (or ensure that the originating agency has attached) to information that will be used, accessed, or disseminated, specific labels and descriptive metadata to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

#### **4.30 Methods of Seeking or Receiving Information**

- a) Information gathering and investigative techniques used by the VIC and participating authorized Agencies will comply with all applicable laws.
- b) The VIC will not directly or indirectly receive, seek, accept, or retain, information from an individual or nongovernmental information provider, commercial database, regardless of whether the entity receives a fee or benefit for providing the information, if the VIC knows or has reason to believe that:
  - i. The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to personnel within the VIC, except if the individual did not act as an agent of or at the direction of any bona fide law enforcement officer participating with the VIC;
  - ii. The individual or information provider used methods for collecting the information that participating center personnel could not legally use, unless the individual did not act as an agent of, or at the direction of any bona fide law enforcement officer participating in the VIC. In this particular case, the Director of the VIC shall seek the advice of the Department's Legal Counsel on the current prevailing state and federal case law on information obtained by a third party individual that is counter to laws of criminal procedure before any information is used;
  - iii. The specific information sought from the individual or information provider could not legally be collected by any participating agency within the VIC; or

iv. The VIC or any of its participating agencies has not taken steps necessary to be authorized to collect the information.

c) The VIC will use the least intrusive information gathering and investigative techniques available in the particular circumstance to gather the information that it is authorized to seek or retain pursuant to Sections 4.10.

d) The VIC 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, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

#### **4.40 Basic Descriptive Information**

The VIC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information should then include:

- a) The name of the originating department, component, and subcomponent;
- b) The name of the agency's justice information system from which the information is disseminated;
- c) The date the information was collected and, when feasible, the date its accuracy was last verified;
- d) The title or position, and contact information for the person to who questions regarding the information should be directed.

#### **4.50 Received Suspicious Activity Reports**

Suspicious activity reports may be received by the VIC. VIC 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 regarding suspicious activity report (SAR) information. Center personnel will:

- a) Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value, and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The VIC will use a standard reporting format and data collection codes for SAR information;
- b) Store the information using the same method as data that rises to the level of reasonable suspicion and shall include an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information;
- c) Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (i.e.: "need-to-know" and "right-to-know" access or dissemination);
- d) Regularly provide access to, or dissemination of, 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.

#### 4.51 Tips and Leads Retention

- a) VIC personnel will retain information only long enough to investigate a tip/lead or SAR information to determine its credibility and value and assign a “disposition” label (i.e.: undetermined or unresolved, cleared or unfounded, or under active investigation) so that an authorized user knows the status and purpose for the retention and will retain the information associated with the disposition label.
- b) VIC personnel will adhere to and follow the VIC’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 equivalent to the system that secures data that rises to the level of reasonable suspicion.

4.52 The VIC will identify and review protected information that is originated from the VIC prior to sharing that information through the ISE. Further, the VIC will provide notice mechanisms, including but not limited to metadata or data field labels, that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with the Department of Homeland Security’s sensitive but unclassified (SBU) or controlled unclassified information (CUI) classifications.

4.53 The VIC’s SAR process provides for human review and vetting to ensure that information is both legally gathered and, when applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

4.54 The VIC’s 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 the 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.

## 5.0 Information Quality

5.10 Information gathering to include acquisition and access, and investigative techniques used by the VIC and authorized agencies providing information to the VIC are required to be in compliance with, and adhere to applicable regulations and guidelines, including, but not limited to:

- a) Vermont Title 20 Chapters 111 and 113;
- b) Applicable criminal intelligence guidelines established under the U.S. Department of Justice’s (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP);
- c) Vermont Rules of Criminal Procedure and all prevailing case law;
- d) 28 C.F.R. Part 23 regarding criminal intelligence information.

- e) The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
  - f) Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
- 5.12 The VIC will make every reasonable effort to ensure that information sought or retained is:
- a) Derived from dependable and trustworthy sources which may include commercial databases in addition to authorized agencies.
  - b) Accurate;
  - c) Current;
  - e) Complete, including the relevant context in which it was sought or received and other related information;
  - f) Merged with other information about the same individual or organization only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
- 5.13 Open Source Information, public information, or a source with an unknown reliability may be used, but it must: 1) be noted as such; and 2) contain a disclaimer that indicates the information may not be accurate and the recipient should independently verify before any action is taken based on the result of the source.
- i. Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.
  - ii. The set of identifying information sufficient to allow merging will consist of available attributes that can contribute to higher accuracy of match, but should have at least three matches.
  - iii. 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
- 5.14 Criminal Intelligence Information will include reliability labeling of source and content validity. All criminal intelligence submission will be reviewed by the VIC, to insure that it meets the requirements of 28 C.F.R. Part 23. The VIC will notify the contributing officer by electronic notification or phone if the report is found not to be in compliance and set a time for correction of information. If the deadline is not met, or the contributor cannot be reached in a timely manner, the information will be deleted without further warning.
- 5.15 At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, timeliness, and confidence (verifiability and reliability)).

- 5.16 The VIC will conduct periodic data quality reviews of information that it generates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the VIC identifies information: 1) that is erroneous, misleading, obsolete, or otherwise unreliable; 2) that the VIC did not have authority to gather the information or to provide the information to another agency; or 3) the VIC used prohibited means to gather the information (except when the VIC's information did not act as the agent of the VIC in gathering the information).
- 5.17 Originating agencies external to the VIC are responsible for reviewing the quality and accuracy of the data provided to the VIC. The VIC 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.
- 5.18 The VIC will make every reasonable effort to ensure that information maintained by the VIC will be corrected when possible or deleted from the VIC's system when the VIC learns that:
- a) The information is erroneous, misleading, obsolete, unreliable, improperly merged or lacks adequate context; such that the rights of the individual may be affected;
  - b) The source of the information did not have authority to gather the information or to provide the information to the VIC, except when the source did not act as an agent to a bona fide law enforcement officer, and only if the rules of criminal procedure and prevailing state and federal case laws allows it, and only after consultation with the Department Legal Counsel;
  - c) The source of the information used prohibited means to gather the information, except when the source did not act as an agent of a bona fide law enforcement officer.
- 5.19 The VIC will advise the appropriate authorized agency who provided the information if its data needs to be corrected or deleted.
- 5.20 The VIC will advise recipient agencies when information previously provided to them is deleted or changed by the VIC 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.
- 5.21 The VIC will establish security safeguards both physical and electronic to ensure that only authorized users are allowed to add, change, or delete information in the databases system maintained by the VIC.

## **6.0 Collation and Analysis of Information**

- 6.10 Collation and analysis
- a) Information as defined by Section 3.0 sought or received by the VIC or from other sources will only be analyzed for purposes defined by Section 4.0:
    - i. By qualified individuals, who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

- ii. To provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities generally and,
- iii. To further crime prevention, enforcement, force deployment, or prosecution objectives and priorities established by the Vermont Department of Public Safety.
- iv. Or for activity which may pose a threat to the public safety as defined in 4.10(a).

b) Information sought or received by the VIC or other sources will not be analyzed or combined in a manner or for a purpose that violates Subsection 4.10

## **7.0 Sharing and Disclosure of Information**

7.10 Credentialed, role-based access criteria will be used by the VIC, as appropriate, to control:

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

7.11 The VIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (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 related to terrorism.

7.12 Information disclosed or shared by the VIC will have labeling consistent DHS classifications.

7.13 Sharing information within the VIC and with other justice system partners

- a) Access to information retained by the VIC will only be provided to persons within the VIC or 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 the law and procedures applicable to the agency for whom the person is working.
- b) An audit trail will be kept of access by, usage, modification and dissemination of information.
- c) Agencies external to the VIC may not disseminate information received from the VIC without prior approval from the originator of the information.

7.14 Sharing information with those responsible for public protection, safety, or public health

- a) The VIC may authorize the release of information retained by the VIC to be disseminated to individuals, as defined in Section 7.13, and individuals in public or private entities,

only for public protection and safety in the performance of official duties in accordance with applicable laws and procedures.

- b) An audit trail will be kept of the access by or dissemination of information to such persons.

#### 7.15 Sharing information for specific purposes

- a) Information gathered and retained by the VIC 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.
- b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
- c) An audit trail of the persons requesting data and of what type of information was disseminated to them will be kept for a minimum of 5 years.

#### 7.16 Disclosing information to the public in the aid of investigation

- a) Information gathered and retained by the VIC may be disclosed to a member of the public or media only if the information meets the legal definition of a non-exempt public record, or if the information can legally be released in the aid of an investigation or public safety as defined by Vermont law. Vermont's public records law is located in Title 1, Chapter 5, Subchapter 3 of the Vermont Statutes. Copies of photographs or imaged likenesses of a person to whom licenses permits or non-driver identification cards have been issued shall not be disclosed except as authorized by 23 V.S.A. § 104.
- b) The VIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
- c) An audit trail will be kept of all requests and of what information is to be disclosed to a member of the public or media

#### 7.17 Information gathered or collected and records retained by the VIC will not be

- a) Sold, published, exchanged, or disclosed for commercial purposes.
- b) Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
- c) Disseminated to persons not authorized to access or use the information.

#### 7.18 Disclosing information to the individual about whom information has been gathered

- a) Upon satisfactory verification of his or her identity and subject to the conditions specified in (c), 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 VIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The VIC's response to the request for information will

be made to the requesting individual by the Department of Public Safety's General Counsel or the VIC Privacy Officer within a reasonable amount of time (thirty (30) days) and in a form that is readily intelligible to the individual. If the information does not originate with the VIC, the requestor will be referred to the originating agency, if appropriate or required, or the VIC will notify the source agency of the request and its determination that disclosure by the VIC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

- b) The existence, content, and source of the information will not be made available to an individual if they are exempt from disclosure under Title 1, Chapter 5, Subchapter 3 of the Vermont Statutes, or if they are exempt from disclosure under Title 9, Chapter 62, Subchapter 3, including situations in which:
  - i. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
  - ii. Disclosure would endanger the health or safety of an individual, organization, or community;
  - iii. The information is in a criminal intelligence system, or;
  - iv. The information relates to 20 V.S.A. § 2056f. (*Dissemination of criminal history records and criminal convictions records to an individual*);
  - v. The information is the property of a source that does not reside within the VIC.
- c) If an individual has objections to the accuracy or completeness of the information retained about him or her, the individual shall submit the objection to the Director of the VIC at the following e-mail address: [DPS.VIC@vermont.gov](mailto:DPS.VIC@vermont.gov). The Commander shall in turn forward the complaint to the VIC Privacy Officer and the Department of Public Safety's General Counsel. The Privacy Officer will notify the person filing the objection that the complaint has been received within thirty (30) days. The individual will be given reasons if requests for correction are denied. The individual will also be informed of the procedure for appeal when the VIC has declined to correct challenged information to the satisfaction of the individual about whom the information relates.
- d) A record will be kept of all requests and of what information is disclosed to an individual.

## 8.0 Information Retention and Destruction

### 8.10 Review of information regarding retention

- a) Intelligence information will be reviewed for purging every five (5) years, or as required by the federal code of regulation, 28 C.F.R. Part 23.
- b) All applicable tips submitted via TipSoft are subject to automatic purging every 60 months (5 years). SAR information will be reviewed for purging at a point no greater than one year. If the information is found to be unsubstantiated, it will be subject to purging as soon as practicable.

- c) A record of information to be reviewed for retention will be maintained by the VIC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.
- d) When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, and deleted, or returned to the submitting source if required.

#### 8.12 Destruction of information

- a) The VIC will delete information, unless it is updated, every five (5) years, and/or as required by 28 C.F.R. Part 23.
- b) A record of information to be purged will be reviewed by the VIC within 30 days of the required purge date.
- c) If the VIC does give prior “Notice of the Pending Purge” or deletion, permission to destroy or return the information record will be presumed if the record is not updated within the specified time period.
- d) To satisfy the integrity and completeness of the purged information from appropriate systems, no record of the purged information will be maintained by the VIC, with the exceptions of information related to subsection 8.13.

#### 8.13 Destruction of classified national security information

Classified information maintained by the VIC that is designated as Secret and above will be audited on an annual basis. This audit will:

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

## 9.0 Accountability and Enforcement

### 9.10 Governance and Oversight

- a) The VIC is overseen and operated by the Vermont State Police. A VSP Lieutenant is assigned as the director of the VIC. A VIC member, sworn or non-sworn will be appointed

by the Lieutenant to serve as the Privacy Officer. The Privacy Officer is responsible for the direct oversight of the privacy policy, which ensures privacy and civil rights are protected.

#### 9.20 Information system transparency

- a. The VIC will be open with the public regarding information and intelligence collection practices. The VIC's web page includes the "Statement of Purpose" as described Section 1.0. The web address for the page is: <http://vsp.vermont.gov/bci/specialinvestigations/vic>
- b. The VIC's privacy policy will be made available upon request. The web page will provide contact information and meet the applicable requirements of Title 1, Chapter 5, Subchapter 3 of the Vermont Statutes.
- c. The Director of the VIC will appoint a Privacy Policy Officer within the VIC to assist in the development and review of this policy and assist with the requirements of section (e).
- d. The Privacy Officer shall be trained as described in Sections 10.0 through 10.30 of this policy.
- e. The Privacy Officer of the VIC will be responsible for the following: 1) community relations; 2) ensuring that privacy and civil rights are protected as provided in this policy and by the VIC's information gathering and collection, retention, and dissemination processes and procedures; and 3) receiving reports regarding alleged errors and violations of the provisions of this policy. The Director and the Privacy Officer will receive and coordinate complaint resolution under the VIC's redress policy, serving as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies, annually reviewing and recommending updates to the policy in response to changes in law and implementation experience, including the results of audits and inspections, and receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the VIC's information system(s). Prior to responding, the Director shall confer with the Department's General Counsel in accordance with Section 5.0. Both the Director and the Privacy Officer can be contacted at the following address: [DPS.VIC@vermont.gov](mailto:DPS.VIC@vermont.gov).
- f. The VIC Director ensures that enforcement procedures and sanctions outlined in 9.30 are adequate, and that procedures are followed and sanctions are enforced.

#### 9.30 Accountability for Activities

- a) The Director of the VIC shall have primary responsibility for the operation of the VIC, it's justice systems, operations, coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, and disclosure of information; and the enforcement of this policy.
- b) The VIC will establish procedures, practices, system protocols, and use of software, information technology tools, and physical security measures that protect the information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The electronic methods and techniques used shall be consistent with that of Vermont Department of

Public Safety Policy and procedural guidelines for general use of systems and internet services. Access to the VIC's databases from outside the facility will be allowed only over secure networks.

- c) The VIC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as designated by the Director of the VIC. The Director will appoint a Security Officer within the VIC to assist with the requirements of sections 9.20(b), (c), (d), (e) and (f).
  - i. The VIC will secure tips, leads, and SAR 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.
- d) The VIC 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. These audits will occur at least annually and a record of the audit will be maintained by the Director (or his designee) of the VIC.
- e) Access to VIC information will be granted only to VIC personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.
- f) To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
- g) The VIC will require all individuals authorized to access the VIC's systems to acknowledge in writing their receipt of the policy and agreement to comply with its provisions.
- h) The VIC personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the VIC's Privacy Officer.
- i) The VIC will annually have an audit and inspection of the information contained in its criminal intelligence system be conducted. This audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the VIC's criminal intelligence system.
- j) The VIC will annually, with additional random checks, review the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to updates in applicable law and public expectations. The VIC shall annually submit a copy of the privacy policy to the Vermont Intelligence Center oversight committee. Acceptance of the review by oversight committee must be granted prior to its implementation. The Director of the VIC will maintain records of the annual review and make them available for the audit when requested.
- k) The VIC or investigating officer, will notify an individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person. The

notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release. Notice need not be given if meets the criteria specified in Subsection 7.50 (b).

- l) 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 and;
    - i. Is held by the VIC and
    - ii. Allegedly has resulted in demonstrable harm to the complainant;
  - c. The VIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the VIC Privacy Officer or Commander at the following address: [DPS.VIC@vermont.gov](mailto:DPS.VIC@vermont.gov) attention Privacy Officer. The Privacy Officer or Director of the VIC 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 VIC the Privacy Officer or Director of the VIC will notify the originating agency in writing or electronically within ten 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 VIC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the VIC will not share the information until such time as the complaint has been resolved. A record will be kept by the VIC of all complaints and the resulting action taken in response to each complaint.
- m) To delineate protected information shared through the ISE from other data, the VIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

#### 9.40 Enforcement

- a) If an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the VIC shall:
  - i. Suspend or discontinue access to information by the VIC personnel, the participating agency, or the authorized user.
  - ii. Apply administrative actions or sanctions as provided by Vermont State Police rules and regulations or as provided in agency personnel policies.

- iii. If user is from an agency external to the Vermont State Police, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions.
- iv. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

#### 9.50 Right to Restrict Access

The VIC 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 accused of violating the VIC's privacy policy.

## 10.0 Training

### 10.1 Personnel requiring training and frequency

- a) The VIC will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:
  - i. All assigned personnel of the VIC.
  - ii. Department personnel providing information technology service to the systems under the VIC's control.
  - iii. Private or commercial personnel providing information technology service to the VIC. This training is not intended to prevent or replace the requirements of Departments VIBRS User agreement.
  - iv. Staff in other public agencies or private contractors providing services to the VIC.
  - v. Users who are not employed by the VIC or a contractor
- b) VIC personnel shall receive policy training during their initial assignment to the VIC and will then receive annual training following the review specified in subsection 9.20(j)
- c) The VIC will provide special training to personnel authorized to share protected information through the ISE regarding the VIC requirements and policies for collection, use and disclosure of protected information.
- d) Personnel within the VIC assigned as the Privacy and/or Security Officer shall receive the additional training appropriate to the position. If the officer is not able to receive the training prior to the appointment, an appointed officer may fill the position. However, all actions will be monitored by the Director of the VIC. This does not preclude receiving the appropriate training as soon as practical.

10.2 Training program content will include:

- a) Purposes of the privacy, civil rights, and civil liberties protection policy; and
- b) Substance and intent of the provisions of the policy relating to the collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the VIC
- c) The impact of improper activities associated with information accessible within or through the VIC; and
- d) The nature and possible sanctions for policy violations, including possible administrative, civil and criminal liability; and
- e) Originating and participating agency responsibilities and obligations under applicable law and policy; and
- f) How to implement the policy in the daily work all users; and
- g) Mechanisms for reporting violations of the VIC privacy protection policies and procedures.

10.30 Record of Training

A record of completion of the initial and annual privacy training and written acknowledgement as described in section 9.20(g) will be maintained by the Privacy Officer.

*Effective August 2010*  
*Revised August 2012*  
*Revised January 2014*  
*Revised July 2016*