Virginia Fusion Center (VFC)
Privacy Policy

A. PURPOSE STATEMENT

The Virginia Fusion Center (VFC) was established in response to the increased need for timely information sharing and exchange of crime and terrorism-related information among members of the law enforcement community. The primary focus of the VFC is the development and dissemination of criminal and/or terrorist related information. This is a process whereby information is collected, integrated, evaluated, analyzed, and disseminated through established procedures for law enforcement purposes and in the interest of public safety. Thereby, intelligence products and services are made available to law enforcement agencies and other entities contributing to public safety throughout the Commonwealth and country.

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

All assigned personnel in the VFC and service users will comply with the VFC privacy policy concerning the information the center collects, receives, maintains, archives, accesses or disclose to center personnel, government agencies, including agencies participating in the Information Sharing Environment (ISE), participating criminal justice and public safety agencies, as well as to private contractors and the general public

The VFC will provide a printed copy of this policy to all assigned personnel in the VFC and will require them to sign a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains. All Service users will be provided a copy of this policy via email and the policy will also be posted to the VFC website.

All VFC personnel, participating agency personnel, private contractors, and other authorized users will comply with all applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to:

The Privacy Act of 1974 – U.S.C Section § 552a as Amended
The U.S. Constitution
The Constitution of Virginia
The following Virginia Code Chapters/Sections:
Virginia Freedom of Information Act, Chapter 37
Disclosure of Criminal records limitations § 2.2-3706
Government Data Collection and Dissemination Practices Act § 2.2-3800
Definitions § 2.2-3801
Systems to which chapter inapplicable § 2.2-3802

Administration of systems including personal information; Internet privacy policy; exceptions § 2.2-3803
Dissemination of reports § 2.2-3805
Rights of data subjects § 2.2-3806
Agencies to report concerning systems operated or developed; publication of information § 2.2-3807
Confidentiality and immunity from service of process; penalties § 52-48
Receipt of Information; immunity from liability § 52-49

All of VFC's criminal intelligence files meeting the standards of collection by the VFC will comply with all internal operational policies and be retained in compliance with Title 28, Code of Federal Regulations, Part 23, the Fusion Center Guidelines and any applicable state or local statutes governing the collection, dissemination, retention, receipt, maintenance, access, and destruction of information. The VFC internal operational policies comply with applicable laws cited in previous paragraph.

C. GOVERNANCE AND OVERSIGHT

The Virginia State Police (VSP) Superintendent's Advisory Board is the management body overseeing the direction of the VFC. The VFC Directors who oversee the day-to-day overall operational responsibility of the center shall be the VSP Criminal Intelligence Division Commander, VSP Criminal Intelligence Division Intelligence Lieutenant, VSP Supervisory Analyst, VSP VFC First Sergeant and the Virginia Department of Emergency Management SACS. The VFC's primary operational responsibilities are its justice systems, operations, coordination of personnel, receiving, seeking, retention, information quality, analysis, destruction, sharing or disclosure of information and privacy policy enforcement. All of these responsibilities are assigned to the VFC's Directors. In order to preserve these rights, VFC has created a legal working group and has designated a Privacy Officer to ensure safeguards and sanctions are in place to protect personal information. The designated and trained privacy official is responsible for handling reported errors and violations, ensuring the provision of training under Section N. of this policy, and, will ensure that the center adheres to the provisions of the ISE Privacy Guidelines and other requirements for participation in the ISE. The legal working group and Privacy Officer are responsible for the development of the privacy policy and annual review. The VFC privacy officer can be contacted at the following email address: vfcprivacyofficial@vsp.virginia.gov.

The VFC has developed, published, and created the following Privacy Policy that sets out standards the VFC will adhere to for the collection, use, and security of information collected in the TIPS, as well as accountability guidelines for the management of such information. The VFC Privacy Policy

incorporates the principles of the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA) and all applicable laws.

The Advisory Board or its designee will take the necessary measures to ensure that access to the VFC's information and intelligence resources is secure. The Board reserves the right to restrict the qualifications and number of personnel having access to the VFC and to suspend or withhold service to any individual or agency violating this Privacy Policy. The Board, or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the VFC.

D. Definitions

Advisory Board: A multi-discipline Advisory Board chaired by the Superintendent of the Virginia State Police and co-chaired by the State Coordinator of Emergency Management tasked with reviewing operational processes and the effective and efficient information management system of the VFC.

C.F.R.: Code of Federal Regulations

Homeland Security Information: any information possessed by federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) 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) a planned or actual response to a terrorist act. [Section 892(f) of the Homeland Security Act of 2002 (codified at 6 U.S.C. § 482(f)(1)].

Information Sharing Environment (ISE): The ISE is a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of criminal activity, including terrorism, against the territory, people, and interests of the United States by the effective and efficient sharing of criminal, terrorism and homeland security information.

Law Enforcement Information—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 Purpose: The request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirm information that requires intervention to prevent a criminal act or threat to public safety and prohibited by state and federal laws and regulations.

Personal Data: Any information relating to an identifiable individual.

Privacy Officer/Custodian of the Records: the person designated by the Criminal Intelligence Division Commander to oversee the VFC's compliance with privacy laws and procedures as well as public records requests.

Reasonable Suspicion/Criminal Predicate: When sufficient facts are established to give a trained law enforcement officer or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise, or terrorism.

Requestor: The individual law enforcement officer or agency making a request for information from, or reporting and incident to, the fusion center; synonymous with "user."

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

Terrorism-Related Information—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential

Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

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

Watch Center: The operations center consisting of analysts, Special Agents, and other supervisors; synonymous with the VFC.

E. Information: Acquiring and Receiving Information

All personal data collected by the VFC will be retained in compliance with the Code of Federal Regulations 28 CFR 23, and Code of Virginia Title 52, Chapter 11, 52-47 thru 52-49, which governs the collection of intelligence and information of the Virginia Fusion Center. Information collected may include the following: law enforcement/investigative information, tips and leads, suspicious activity reports (SARs), classified and non-classified reporting, and public records. The VFC will also adhere to criminal intelligence collection guidelines established under the National Criminal Intelligence Sharing Plan (NCISP). The VFC has a separate Suspicious Activity Reporting (SAR) privacy policy that is included as an Appendix to this overall policy and includes the following: Receipt and collection, Assessment of credibility and value, storage, access and dissemination and retention and security of the information.

The VFC will ensure that information is categorized, labeled and classified to the maximum extent feasible, to reflect any limitations on disclosure based on sensitivity of disclosure, in order to:

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

The VFC will only seek and/or retain information, except as noted below, on individuals and organizations when there is a reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is planning criminal conduct or activity (including terrorism) that presents a threat to any individual, the community, or the nation, and the information is relevant to the criminal conduct or activity. Further, the VFC will only seek information on individuals and organizations in response to requests for support from field operating elements engaged in an ongoing law enforcement investigation or event, and/or non law enforcement agencies/entities for health and public safety purposes.

The VFC will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information.

The VFC will not seek information about an individual or organization solely on the basis of their religious, social or political views, or their race, ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation.

The VFC will contract only with commercial database entities that demonstrate that they gather personally identifiable information in compliance with local, state, tribal, territorial, and federal laws and which is not based on misleading information collection practices.

Information gathering and investigative techniques used by the VFC will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

Nothing in this paragraph shall be construed to limit the ability of the VFC Watch Center to initiate, without a specific request, short term research or information gathering regarding events or activities being publicly reported in the media which may impact on the health and public safety of the Commonwealth of Virginia.

Stakeholder agencies are responsible for ensuring the legal validity of gathered information to include the following minimal guidelines.

1. The source of the information is reliable and verifiable.

2. Information supports reasonable suspicion the individual or organization is involved in criminal conduct, and the information is relevant to that conduct.

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

4. Information may not be collected concerning political, religious or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation or social views, associations, or activities of any individual, group, or organization unless the information directly relates to criminal conduct or activity, and there is reasonable suspicion the subject is involved in the illegal conduct.

5. Information accurately reflects what was reported by the source of information.

6. Information that does not appear to meet the criteria set fourth above shall be reviewed by a supervisor of the VFC for determination as to whether or not the information should be collected by the VFC. Such review may include further investigation into the credibility of the information.

The VFC will abide by daily operating procedures for the initial collection and verification of criminal intelligence and information, including the screening process by an analyst/agent/call taker and the subsequent review by supervisory personnel. A trained analyst in the watch center will review the submitted information and intelligence and will make a determination on the validity and reliability of the information or intelligence and this will clearly be marked on the report. In addition, the report will be clearly marked as it relates to the nature and purpose of the report.

The VFC is maintained for the purpose of developing information and intelligence for and by participating stakeholder agencies. The decision of the agencies to participate with the VFC and to decide which databases to provide for VFC access is voluntary and will be governed by the laws and rules governing those individual agencies, as well as by applicable federal laws.

The VFC Watch Center is generally responsible for the receipt and collection of information directed towards specific person, businesses, or groups where there is reasonable suspicion (as defined in 28 CFR, Part 23) that the individuals or organizations are involved in terrorism or other criminal activity. In addition, personnel in the watch center collect non-criminal homeland security related information that can be utilized to assess risks, threats, and vulnerability of the Commonwealth. The collection, storage, and

dissemination of criminal and homeland security intelligence information by the VFC adhere to the privacy and constitutional rights of individuals, groups, and organizations.

After information has been evaluated, the Watch Center employee determines the classification of the information. Information that is already classified by another agency shall remain at that classification. The classification category to which the information is placed shall remain at that classification. The classification category to which the information is placed shall also determine how the information is handled, disseminated, and filed. Once information is classified by the Watch Center employee, it shall remain in that classification unless additional information arises and is authorized by a VFC Director to reclassify or declassify such information. The classifications used by the VFC include the following: Law Enforcement Sensitive (LES), For Official Use Only (FOUO) and Open Source (OS). Only those stakeholders that have a "right" and "need" for this information contained in these classifications will receive the information.

For purposes of sharing information in the ISE, all information reports will clearly indicate if the report contains protected information that includes information about U.S. citizens, lawful permanent residence, or personally identifiable information. These reports also will include information disclaimers, labels and descriptive information that indicate the proper handling of the information/intelligence, legal authority and penalties for the mishandling of information/intelligence and information/intelligence sharing based on information/intelligence sensitivity and classification. The VFC requires certain basic, descriptive information (metadata) to be entered and associated with each record, data set, or systems of records containing personally identifiable information that will be accessed, used, and disclosed within the ISE.

To delineate ISE information from other data, the VFC maintains records of the ISE originating agencies the center has access to, as well as audit logs, and employs system mechanisms whereby the sources is identified within the information record.

Any violations of the Virginia Fusion Center Privacy Policy will be addressed by the VSP Criminal Intelligence Division Commander.

F. Information Quality Assurance

Stakeholder agencies participating in the VFC, including agencies participating in the ISE and providing data remain the owners of the data contributed. These agencies are responsible for the quality and accuracy of the data accessed by the Watch Center. At the time of retention in the

system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence. The VFC will advise the appropriate data owner, in writing if its data is found to be inaccurate, incomplete, out of date or unverifiable.

The ISE requires that originating agencies providing data to the VFC be advised in writing if their data is found to be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected. If the information is determined to be erroneous, the information will corrected if appropriate, deleted if it has been found to be erroneous and no further action is possible or the center will refrain from using the information. VFC personnel will endeavor to ensure the accuracy of information received through database searches, by cross-checks with other data systems and open source information. In order to maintain the integrity of the Watch Center, any information obtained through the Watch Center will be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data. When personnel within the VFC receive information from outside agencies or the public, they will assess the reliability (Reliable, Unreliable, Unknown) and the validity (Confirmed, Doubtful, Unverified) and these labels shall be placed on the report. If the Center receives additional information or additional information is gathered that impacts the confidence of the information, the center will reevaluate and revise or amend the labeling if needed.

VFC management is responsible for the quality and accuracy of records that the VFC creates or modifies. VFC management is responsible for researching suspected errors and deficiencies. If the information is determined to be erroneous, the information will corrected if appropriate, deleted if it has been found to be erroneous and no further action is possible or the center will refrain from using the information.

In accordance with 28 CFR Part 23 standards, when criminal Intelligence information has no further value or meets the criteria for removal under applicable law or regulation, it will be purged, destroyed, deleted, or returned to the submitting source. Criminal intelligence information will also be reviewed within five years from the submission date or last validation of the information. Personnel shall run criminal history checks on subjects to determine if they have had any criminal activity in the past five years. If the information cannot be substantiated for suspected involvement in current criminal activity, it shall be purged from both computer storage media and hard copy paper records shall be destroyed. If substantiated, it will be validated for an additional 5-year retention period.

In accordance with the Code of Virginia, Title 52, Chapter 11, 52-48, the department shall also conduct an annual review of information contained in any database maintained by the VFC. Data that has been determined to not have a nexus to terrorist activity shall be removed from such database. A reasonable suspicion standard shall be applied when determining whether or not information has a nexus to terrorist activity. If the VFC has data that may be inaccurate or incomplete, incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected, this information shall be corrected or purged from any VFC database.

In addition, if inaccurate or incomplete, incorrectly merged information, is out of date, cannot be verified, or lacks adequate context that the rights of the individual may be affected, is provided to participating agencies, the VFC will notify those participating agencies that received the initial report.

In addition, the VFC will also conduct an evaluation of all information to determine the source's reliability and validity, timeliness of the information, and consistency with previous reporting. If it is determined that the source is not credible, the information is not relevant or current, or the information does not support the overall mission, it will be forwarded to the Analyst Supervisor for additional evaluation.

G. Collation And Analysis

Information obtained from or through the VFC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirm information that requires intervention to prevent a criminal act or threat to public safety and prohibited by state and federal laws and regulations. Information acquired by the VFC or accessed from other sources will only be analyzed by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable and have been selected, approved, and trained accordingly. Information subject to collation and analysis is information defined and identified in Section E, Information: Acquiring and Receiving Information.

The VFC Advisory Board or designee will take necessary measures to ensure access to the Watch Center's information and intelligence resources is secure. Unauthorized access or use of the resources is forbidden. The Board reserves the right to restrict the qualifications and number of personnel having access to the Watch Center and to suspend or withhold service to any individual violating the Privacy Policy. The Board, or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the Watch Center.

Information disseminated by the VFC will be authorized on a "need to know" and "right to know" basis, and will be provided in accordance with applicable laws, rules, and regulations. Access to information gathered or retained by the VFC will only be provided to persons within the VFC or within other criminal justice, public safety, or regulatory agencies who are authorized access and only for legitimate law enforcement, public protection, prosecution, or other justice purposes, and only for the performance of official duties in accordance with applicable laws and procedures. All documents sent out by the VFC will contain a legal restriction attachment protected by The Code of Virginia, Title 52-48 and 52-49. All information reports that are disseminated to Law Enforcement Agencies that contain U.S. person identifiable information will be clearly marked indicating the report contains U.S. person information. In addition, the report will contain a disclaimer advising how to handle the information within their Department. In addition, any Law Enforcement Agency that receives these report's, must have a signed VFC non-disclosure agreement on file that outlines the proper handling of the report and penalties for the dissemination to unauthorized users that do not have a "right" or "need" for the information report.

In accordance with established VFC Standard Operating Procedures, an audit trail will be kept of access by or dissemination of information to such entities. Furthermore, all personnel who receive, handle, or have access to Watch Center data will be trained as to those regulations on security policy procedures and the VFC Privacy Policy to ensure that there are no security breeches and that all applicable laws and regulations of individuals and organizations' are protected. All personnel having access to VFC data agree to abide by the following rules:

1. The VFC's data will be used only in support of official law enforcement activities in a manner authorized by the requestor's employer.
2. Individual passwords will not be disclosed to any other person, except as authorized by VFC management.
3. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
4. Background checks will be completed on personnel who will have direct access to the VFC at a level determined by the Advisory Board or their designee.
5. Use of the VFC data in an unauthorized or illegal manner will subject the requestor to denial of further use of the VFC, discipline by the requestor's employing agency, and/or criminal prosecution.

Information gathered or retained by the VFC may be disseminated to non-criminal justice public or private entities only for public protection, critical infrastructure protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable law and

procedures. In accordance with established VFC Standard Operating Procedures, an audit trail will be kept of access by or dissemination of information to such entities.

The VFC reserves the right to deny access to any VFC user who fails to comply with applicable restrictions and limitations of the VFC policy.

H. Merging Records

Records 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. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match. 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.

I. Sharing and Disclosure

Credentialed, role-based access criteria will be used to control: what information a class of users can have access to; what information a class of users can add, change, delete or print, and to whom the information can be disclosed and under what circumstances.

Access to or disclosure of records retained by the VFC will only be provided to persons within the VFC or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for whom the person is working. An audit trail will be kept of access by or dissemination of information to such persons.

Participating agencies may not disseminate VFC information received from VFC without approval from the originator of the information.

Stakeholder agencies participating in the VFC and providing data to/through TIPS remain the owners of the data contributed. These agencies are responsible for the quality and accuracy of the data accessed by the VFC. VFC personnel will endeavor to identify inconsistencies between information received through databases searches and information crosschecked with other data systems and open source information in a manner consistent with

the Standard Operating Procedures. User agencies and individual users are responsible for the purging and updating of the data provided to the VFC.

Information obtained from or through the VFC can only be used for lawful purposes.

A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal or terrorism investigation, or is intended to assist in an intervention to prevent a possible criminal/terrorist act or threat to public safety.

Unauthorized access or use of the VFC information resources is forbidden.

User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information.

Information gathered and records retained by VFC may be accessed or 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. Requests for information under the Virginia Freedom of Information Act, requests for correction to information disclosed, and appeal procedures are detailed at http://www.vsp.state.va.us/Freedom_of_Information.shtm.

All Information and intelligence gathered or collected and records retained by the VFC may be accessed or 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 VFC mission and is not exempt from disclosure by law. Such information may only be disclosed in accordance with the law and procedures applicable to the VFC for this type of information. See §2.2-3706, §2.2-3802, §52-48, and §52-49 of the Code of Virginia.

Information and intelligence gathered and records retained by the VFC will not be provided to the public if, pursuant applicable law, it is:

- Required to be kept confidential or exempt from disclosure pursuant to §52-48 Code of Virginia.
- Classified as investigatory records and exempt from disclosure pursuant to §2.2-3706 Code of Virginia.
- Protected federal, state, tribal records originated and controlled by the source agency that cannot be shared without permission or exempt from disclosure pursuant to §52-48 Code of Virginia.
- A violation of an authorized nondisclosure agreement or exempt from disclosure pursuant to §52-48 Code of Virginia.

Information obtained from or through the VFC will not be used or publicly disclosed for purposes other than those specified in the Memorandum of

Understanding or Non-disclosure agreement signed with the participating agency.

Regardless of the Memorandum of Understanding or Non-disclosure agreement, information and intelligence cannot be:

1. Sold, published, exchanged, or disclosed for commercial purposes;
2. Disclosed or published without prior approval of the contributing agency (with the exception of information released through Public Records Act requests and/or other disclosures required by applicable law); or
3. Disseminated to unauthorized persons.

The VFC will not confirm the existence or nonexistence of Information and intelligence gathered and records retained by the VFC to any person, organization, or other entity not otherwise entitled to receive the information, unless otherwise required by law.

If an individual has a complaint or objection to the accuracy or completeness of information about him or her that originates with another agency, the VFC's Director or designee will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction 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, remove the record, or assert a basis for denial in accordance with Virginia Code § 2.2-3800. This must be done in sufficient time to permit compliance with deadlines found within Virginia Code § 2.2-3800. A record will be kept of all complaints and correction requests.

J. Redress (complaint and correction when no right to disclosure) Chapter 38 of Title 2.2 Code of Virginia.

The VFC has adopted redress procedures pursuant to the ISE Privacy Guidelines for situations when a complaint involves records that have not been disclosed to the complainant under applicable law.

- If an individual has complaints or objections to the accuracy or completeness of Information and intelligence gathered and records retained by the VFC about him or her that is alleged to be held by the VFC, the VFC, as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

- The VFC will acknowledge the complaint and state that it will be reviewed but will not confirm the existence of any Information and intelligence gathered and records retained by the VFC that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from any VFC database if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.
- If an individual has complaints or objections to the accuracy or completeness of ISE information that has been disclosed to him or her the VFC ISE privacy official or designee will notify the originating ISE agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. The originating ISE agency must consent to the correction, remove the record, or assert a basis for denial in accordance with Virginia Code 2.2-3800. This must be done in sufficient time to permit compliance with deadlines found within Virginia Code 2.2-3800. A record will be kept of all complaints and correction requests.
- Any complaints, Redress or inquiries can be addressed to the privacy officer at the following email address: vfcprivacyofficial@vsp.virginia.gov

K. Security Safeguards

A Special Agent assigned to the Virginia Fusion Center shall be designated and trained to serve as the VFC's security officer.

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

The Board or its designee will identify technical resources to establish a secure facility for VFC operations with restricted electronic access, security cameras, and alarm systems to guard against external breach of the facility. In addition, the Board or its designee will identify technological support to develop secure internal and external safeguards against network intrusion of VFC data systems. Access to the VFC databases from outside of the facility will only be allowed over secure network lines.

The VFC 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.

Research of the VFC's data sources is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the VFC will be granted only to fully authorized personnel who have been screened with state and national fingerprint-based

background checks, as well as any additional background standards established by the VFC Advisory Board.

The VFC personnel or other authorized users may report violations or suspected violations of center policies relating to protected information to the VFC Privacy Officer for action up to and including revocation of the users memorandum of understanding or Non-disclosure agreement and reporting to VFC Management.

The VFC will consider notifying an individual about whom personal information was or is reasonably believed to be breached or obtained by an unauthorized person and access to which threatens the physical, reputation, or financial harm to the person. Any notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the 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, or the VFC will follow the guidelines set forth in Office of Management and Budget (OMB) Memorandum M-07-16 (May 2007).

L. Information Retention and Destruction For Criminal Intelligence Information

All applicable information will be reviewed for intelligence record retention (validation or purge) annually as provided by Virginia Code § 52-48 and § 52-49.

When information has no further value or meets the criteria for removal according to the VFC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting source.

The VFC will delete information or return it to its source, unless it is validated, annually, which will be compliant with Virginia Code § 52-48 and § 52-49.

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

Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and any agreement with the providing agency.

A record of information to be reviewed for retention will be maintained by the VFC and for the appropriate system (s), notice will be given to the submitter at least thirty (30) days prior to the required review and validation/purge date.

M. Transparency, Accountability and Enforcement

It is the intent of the VFC and participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the originating agency of information as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an inquiry or investigation. All other inquiries shall be referred to the Privacy Officer/Custodian of the Records.

The VFC will post this Privacy Policy on the public web site of the Virginia Fusion Center and make it available to any interested party.

The VFC will have access to an audit trail of inquiries that identifies the inquirer and information disseminated from VFC data applications.

The VFC data logs will be utilized to maintain an audit trail of requested or disseminated information.

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

The VFC 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.

The VFC will adopt and follow procedures and practices to evaluate the compliance of its authorized users with their systems, in provisions of this policy and applicable law. This will include periodic and random audits of these systems, as to not establish a pattern of the audits. The VFC will conduct periodic audit and inspection of these systems. The audit will be conducted by VFC staff or an independent auditor. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the information maintained by the VFC in these systems and any related documentation. The VFC's personnel or other authorized users may report violations or suspected violations of center policies relating to protected information to the center's Privacy Officer.

Failure to abide by the restrictions for the use of VFC data may result in the suspension or termination of user privileges; discipline imposed by the user's

employing agency, and/or criminal prosecution. Sanctions are under the authority of the VSP Criminal Intelligence Division Commander, who shall be assisted by the Privacy Officer.

The VFC's Legal Workgroup, under the guidance of the Privacy Officer, will periodically review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems and changes in public expectations.

N. Training

The VFC 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:

- All assigned personnel of the center
- Personnel providing information technology service to the VFC
- Staff in other public agencies or private contractors providing service to the agency, and
- Users who are not employed by the agency or contractor.

The VFC will provide special training to personnel authorized to share protected information in the Information Sharing Environment regarding the center's requirements and policies for collection, use, and disclosure of protected information.

The VFC's privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy;
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the VFC;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improving activities associated with an infraction accessible within or throughout the agency;
- Mechanisms for reporting violations or center privacy-protection policies; and,
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability and immunity, if any.