



# State of Vermont - Department of Public Safety

## VIBRS User Agreement & Account Request Form

### VIBRS User Policy

Policy # 95-3  
Version Adopted:  
Nov. 2, 2011

VIBRS User Policy  
Division of Criminal Justice Services  
For the VIBRS Advisory Board

Note : This is a mandatory policy.

#### 1. Vermont Incident Based Reporting System (VIBRS) Network GOALS

- 1.1 To provide a network that will deliver a variety of applications and services for the effective and efficient administration of justice to include but not limited to, criminal history information, access to NCIC and NLETS, and intelligence information.
- 1.2 To operate a secure automated Computer Aided Dispatch and Records Management system that gathers data for a variety of criminal justice purposes, including but not limited to, incident/event information, arrest information, stolen property information and crime data information.
- 1.3 To capture all contacts a person has with law enforcement and disseminate that information to contributing and non-contributing agencies for the purposes of crime prevention, crime detection, officer safety, investigative inquiry, management information, crime analysis purposes, and background information.
- 1.4 To provide statistical reports relating to the above information. This will allow the user the opportunity to respond to questions relating to crime activity in their communities and to provide information that will allow them to make better decisions regarding the operations of their agencies.
- 1.5 To provide an alternative, cost effective and efficient means of communication between users and agencies or persons that have access to electronic mail.

#### 2. Definitions

Agency - An agency as used in these policies is a department(s) that have a federal ORI number and whose mission/purpose/focus is the investigation and /or prosecution of criminal activity.

CJS IT Staff - Information technology staff that work for the Department of Public Safety, division of Criminal Justice Services.

Contributing Agency - A contributing agency is an agency that uses the Vermont Incident Based Reporting System CAD/RM system, entering and contributing information into the system for the purposes of NIBRS reporting, agency administration and law enforcement investigative purposes.

Non-Contributing Agency - A non-contributing agency is an agency that uses the Vermont Incident Based Reporting System CAD/RM system for law enforcement investigative purposes and does not enter information.

Personal Identifying Information - Personally identifiable information is one or more pieces of information, when considered together, or combined with other information, and when considered in the context of how it is presented or how it is gathered, is sufficient to specify a unique individual.

Records Management - A term used to describe the law incident data collected by a law enforcement agency.

Site - a site is a location where a network connection is located or where access to the network is allowed this also includes wireless connections. Most agency offices are sites and some agencies may have more than one site.

Tech Liaison - A representative from a user agency that is one of the agencies employees. This person will interface with the staff at the user agency, as well as become the point of contact with CJS IT staff. The tech liaison will be the point of contact for the user agencies staff to contact first and will refer IT network problems to the CJS IT Staff.

User - A user is an individual authorized by an agency head to have access to the information contained in the databases of the VIBRS network. The user must be under the employment of the agency head or under contract or agreement where the agency head has the ability to monitor the user's use of the network.

VIBRS Advisory Policy Board - A board made up of VIBRS network users and others that is created to provide advice and counsel to the Division of Criminal Justice Services of the Vermont Department of Public Safety regarding the operation of the VIBRS network.

VIBRS CAD/RMS - The Vermont Incident Based Reporting System (VIBRS) Computer Aided Dispatch (CAD)/Records Management System (RMS) is a database that is used by contributing agencies for the collection of law enforcement incident information. The software is provided by Spillman Technologies Inc, and the system is sometimes referred to as "Spillman".

VIBRS Network - The VIBRS network is a proprietary confidential and secure network, managed by the State of VT Department of Public Safety. Because of its data sharing capabilities it is for law enforcement and justice related use only and is not for personal use. The VIBRS network is a portal into a system of services that includes several law enforcement and related databases. These databases and services include but are not limited to:

- VIBRS Computer Aided Dispatch (CAD)/Record Management System (RMS)
- Vermont law Enforcement Telecommunication System (VLETS), which is a system allowing access into a variety of national and state databases.
- Vermont Justice Information Sharing System (VJISS)

#### 3. Collection of Information within the VIBRS network and VIBRS CAD/RMS.

3.1 A user shall only collect that information that pertains to the management of activities and records for their agency as authorized by the agency head and by law. This information shall include information that is:

3.1.1 Collected by law enforcement officers on all persons who have contacts with law enforcement agencies. This contact may be self generated by the law enforcement officer or from a call for service by a person. Information may include personal identifying information from the person who contacts the department or agency.

3.2 A user or their department/agency shall not collect or retain information about an individual or organization solely on the basis of their religious, political or social views, their participation in a particular organization, or because of their race, ethnicity, place of origin, sex , or sexual orientation. Such information can be sought and retained if it is:

3.2.1 Needed by the agency to identify an individual for the agency's effective operation.

3.3 A user who collects and retains information shall comply with all applicable laws relating to the collection of information for the purposes of law enforcement records management.

3.4 Information that is collected as authorized by law.



# State of Vermont - Department of Public Safety

## VIBRS User Agreement & Account Request Form

### VIBRS User Policy

#### 4. Use Limitations

4.1 All data residing on the VIBRS network is the property of the agencies participating in the VIBRS network. Summary information of involvements contained within the names table of the record management systems may be released to law enforcement agencies for law enforcement purposes. The user who chooses to release such data may do so only by telling the law enforcement agency that a law enforcement involvement exists and directing the inquirer to the owner of the involvement data.

4.2 Agencies of the VIBRS network may choose to allow other VIBRS agencies to have "view only" access to their records management law incident data. The user must understand that information viewed may be in draft form.

4.3 All law incident data residing in the VIBRS network is the property of the contributing agencies. Prior approval, in writing (to include e-mail), from the originating agency must be obtained before any specific information about the involvement may be released (verbally or in print). In extraordinary cases involving officer safety information may be released if it is needed to protect an officer.

4.4 Personal identifying information within the VIBRS CAD/RMS shall belong to all users and is the property of the system and may be released or disseminated for law enforcement purposes, only. Examples of such personal identifying information may include but is not limited to: Dates of birth, Place of birth, Address and phone number, SSN.

4.5 Personal identifying information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed, released, disseminated or used for personal purposes, (3) disseminated to unauthorized persons. A violation of this section may result in sanctions as stipulated in Section 12 of this policy and may result in criminal prosecution for violating relevant criminal laws.

4.6 Use of the information contained in the VIBRS network databases is for law enforcement purposes or justice purposes only and shall only be released or disseminated in accordance with these policies or policies associated with the operation of VLETS. Any use and dissemination of information in the VIBRS or VLETS databases for personal or financial gain is strictly prohibited and may be subject to criminal prosecution (theft of services) and loss of access privileges for the user and agency.

#### 5. Site Security

##### 5.1 Users

5.1.1 A user shall not add hardware or software that allows unauthorized access to the VIBRS network.

5.1.2 A user that poses a security risk to the VIBRS network as determined by their department head, CJS staff or the VIBRS Advisory Policy Board may be disconnected or have their access privileges removed until security risks have been minimized.

6.1 Only activities that relate to public safety, law enforcement or criminal justice shall be allowed on the VIBRS system. Each user is to be

5.2.1 The department head of a contributing or non-contributing agency shall ensure that all aspects of the FBI CJIS Security Policy are met with regards to physical site security.

#### 6. System Usage

6.1 Only activities that relate to public safety, law enforcement or criminal justice shall be allowed on the VIBRS system. Each user is to be familiar with VIBRS POLICY 01-01, Electronic communications and internet use. Failure to comply with this policy may result in the implementation of sanctions contained in Section 12.

6.2 Each site and user shall make a reasonable effort to minimize their impact on the system.

6.3 Recognizing the need for data integrity it is strictly prohibited for any user to intentionally modify system data in such a way that it would make the data erroneous or inappropriate in nature. Any user who modifies data inappropriately may be subject to sanctions contained in Section 12 and may be subject to criminal prosecution.

#### 7. Policy Review

7.1 This policy shall be reviewed by the VIBRS Advisory Board annually, or as required.

#### 8. Email

8.1 E mail sent to an individual user is not to be considered "Confidential." However, no one should look at another person's e-mail unless they have permission from that user or the person is the user's supervisor and the supervisor has cause within the limits of his/her supervisory authority.

8.2 E mail groups are subject to change without notice. If you must be certain of the recipients of an e mail message, do not use an e mail group. E mail that is sent to an e mail group should be considered the same as a posting on a bulletin board.

8.3 The e mail system is for the free use of VIBRS users with the following restrictions:

8.3.1 Offensive material is not allowed.

8.3.2 Users shall restrict the use of e mail to official business as determined by their agency head. These restrictions shall include but not be limited to:

8.3.2.1 Lobbying public officials or asking others to lobby in their behalf.

8.3.2.2 Printing and/or distributing information from the Internet that is obscene, potentially offensive, harassing or disruptive.

8.3.2.3 Using or allowing others to use Internet services or e-mail accounts to conduct transactions or advertising for a personal profit making business.

8.3.3 Users shall take reasonable measures to limit the amount of e mail they generate.

8.3.4 Users should be aware that system backups would contain copies of e mail messages. Deletion of an e mail message does not guarantee that all copies of the message have been erased.

8.3.5 Users should be aware that the contents of e mail could be used as evidence in civil, criminal and internal investigations. Therefore, e-mail should not contain any material, which can be construed to indicate bias, prejudice or any other litigation liability, which may be damaging to the departments that use the VIBRS network.

8.3.6 Users should never include their password or any other security related information in an e mail message.

8.3.7 No employee shall send e-mail that is, or appears to be, sent from another employee's e-mail or that attempts to mask identity.

#### 9. System Security

9.1 Although reasonable efforts are taken to insure system security, absolute security cannot be guaranteed. Therefore, the following material should be stored on the VIBRS network at the user's discretion:

9.1.1 Any investigative work which if compromised would jeopardize the outcome of a criminal investigation.

9.1.2 Information, which if compromised, would place an individual in jeopardy. This would include the names of informants.



# State of Vermont - Department of Public Safety

## VIBRS User Agreement & Account Request Form

### VIBRS User Policy

9.2 The CJS staff shall assign each authorized user a unique login name and will require that user to select a password.

9.3 Users shall not allow another individual to use their login or password. A login may be kept open if a supervisor authorizes a user to keep their login open, due to exceptional circumstances, for the purposes of maintaining the police operation. A password shall never be shared.

9.4 Users shall report any suspicious system activity to the agency technical liaison.

9.5 Users shall not give out system or site related information.

9.6 Users shall not leave a logged in terminal or workstation unattended or unlocked.

9.7 Users shall not place hardware or software on any device that is connected to the VIBRS network that may compromise the security of the network. Examples may include but are not limited to internet usage surveillance software that logs key strokes.

#### 10. Passwords

10.1 All logging of system activity is based on login and password. You may be held responsible for anything that takes place through your login. DO NOT REVEAL YOUR PASSWORD TO ANYONE FOR ANY REASON. Do not allow anyone to use your login and password unless authorized by VIBRS policies. CJS staff members will NEVER need to ask you for your password.

10.2 Never put your password in a document stored on the computer system.

10.3 All users are required to have a password. New accounts will be issued a password for themselves the first time they log on. You may be required to periodically change your password.

10.4 If you feel that the secrecy of your password has been compromised, have it changed immediately by notifying your technical liaison.

10.5 If you forget your password, notify your Technical Liaison. The Technical Liaison must then e mail the CJS staff with the login of the person who needs a new password and a time they may be reached by phone. A VIBRS staff member will then securely transmit the new password to the user.

#### 11. Policies

11.1 The CJS STAFF of the Division of Criminal Justice Services reserves the right, upon a recommendation of the Advisory Policy Board, to adopt rules, policies and procedures relating to the input, control and integrity of the data contained within the VIBRS network databases.

11.1.1 These rules, policies and procedures shall be in the form of mandatory and recommended rules, policies and procedures.

11.1.2 Failure of agencies and users to adhere to mandatory rules, policies and procedures will result in sanctions levied against the individual user and/or agency as described in Section 13 and could include criminal prosecution.

#### 12. Acknowledgements

12.1 The CJS staff reserves the right to monitor the system.

12.2. The CJS staff reserves the right to make changes to this document where it can be shown that such changes are needed in order to insure system security and availability. A copy of any such changes will be sent to the VIBRS Advisory Board for ratification.

12.3 Users shall report any system problems to the CJS staff by sending e mail to "help" or by calling DPS Headquarters at 241 5599.

12.3.1 Users are encouraged to first contact their technical liaison to try and first resolve problems.

12.4 Users shall not attempt to change any system setting or perform any system modifications or repairs without the approval of the CJS staff.

12.5 Occasionally the system will need to be brought down for maintenance. Advance notice will be given where practical. All users must be logged off by the time specified. Users who are not logged off may be logged off without notice and data loss may result.

12.6 Users shall not place any material on the VIBRS network unless they are legally permitted to do so. This specifically includes non public domain software and any other licensed intellectual properties.

#### 13. Sanctions

13.1 Agencies and users of the VIBRS Network shall adhere to this policy and any other mandatory rule, policy or procedure of the VIBRS network. Failure to do so may result in the user or agency being sanctioned by the VIBRS staff of the Division of Criminal Justice Services as deemed appropriate by the VIBRS Advisory Board.

13.1.1 A user's conduct or behavior, as determined by the VIBRS Advisory Board that threatens the security or integrity of the data within the network may result in a user being sanctioned as deemed appropriate by the VIBRS Advisory Board.

13.2 Sanctions could result in a loss of privileges (disconnection) by the agency or user and may be subject to civil and/or criminal liability and/or prosecution in state and/or federal court.

13.3 The CJS staff may impose emergency sanctions, including disconnection, if they believe there is a security threat sufficient to warrant such action. The disconnection will be subject to the review and concurrence of the VIBRS Advisory Board.



# State of Vermont - Department of Public Safety

## VIBRS User Agreement & Account Request Form

### VJISS User Policy

1. In addition to the items terms listed within this policy, authorized VJISS Users are also bound by any terms or conditions found within the VJISS Privacy policy as listed on the VJISS system pages.

#### 2. Vermont Justice Information Sharing System (VJISS) GOALS

2.1 To operate a secure automated Vermont Justice Information sharing system that provides data for a variety of criminal justice purposes, including but not limited to, incident/event information, arrest information, and crime data information.

2.2 Currently the VJISS System provides a query tool that searches CAD/RMS systems of Vermont police agencies. The system queries name records, vehicle records, incident locations, and incident numbers. It is a federated searching system, which means that VJISS only provides a look into the contributing CAD/RMS systems and does not store information into a database. This allows for agencies to have control over their systems and provides for real-time searching of information.

#### 3. Legal Compliance

3.1 All participating agency personnel, personnel providing information technology (IT) services to the contributing agencies and DPS, private contractors, and users will comply with all laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

#### 4. Definitions

Agency - An agency as used in these policies is a department(s) that has a federal ORI (Originating Reporting Identifier) number and whose mission/purpose/focus is the investigation and /or prosecution of criminal activity.

Contributing Agency - A contributing agency is an agency that contributes information from its own CAD/RMS into VJISS.

CAD/RMS - Is an acronym for computer aided dispatch and records management system. Within this policy the term CAD/RMS means the same.

Non-Contributing Agency - For the purposes of this policy, a non-contributing agency is an agency that does not contribute information to one or more of the databases accessible for query within the VJISS system and who uses the system for criminal investigative purposes.

Disseminate - To spread, release, or disperse information from the CAD/RMS to anyone.

Information - Includes individual pieces of or collections of pieces of data about people, organizations, events, incidents, objects, real or personal property, whether in physical, manual, or electronic form, including documents, writings, electronic representations of text or graphic documents; an electronic image including a video image, of document evidence, object or event; information in the fields or files of an electronic database, or an audio or video recording, analog or digital, of an event, or notes in an electronic file from which a transcript of an event can be prepared.

Law - As used in this policy, "law" includes any federal, state, local, or tribal statute, ordinance, regulation, executive order, or court rule, decision, or order, as construed by appropriate federal, state, tribal, or local officials or agencies.

User - A user is an individual authorized by the head of an agency to have access to the information contained in the databases of VJISS. The user must be under the employment of the agency head or under contract or agreement where the agency head has the ability to monitor the user's utilization of the network

#### 5. Disclosure of Information According to Originating Agencies' Access Rules or Policies

5.1 All law incident data residing in VJISS is the property of the contributing agencies. Prior approval, in writing (to include e-mail), from the originating agency must be obtained before any specific information about any involvement may be released (verbally or in print). In extraordinary cases involving officer safety information may be released if it is needed to protect an officer.

5.2 Summary information of involvements contained within the names table of the record management systems may be disseminated to law enforcement agencies for law enforcement purposes. The user who chooses to release such data without prior approval in writing, may do so only by telling the law enforcement agency they are disseminating to that a law enforcement involvement exists and directing the inquirer to the owner of the involvement data.

5.3 VJISS and its users will only seek information that is collected by law enforcement officers on persons who have contact with law enforcement agencies and is stored or placed lawfully into agencies' databases in accordance with those agencies' policies.

5.4 Personal identifying information within the VJISS system shall belong to all users and is the property of the system and may be released or disseminated for law enforcement purposes, only. Personal identifying information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed, released, disseminated or used for personal purposes, (3) disseminated to unauthorized persons. Examples of such personal identifying information may include but is not limited to: Dates of birth , Place of birth , Address and phone number , SSN.

5.5 Use of information contained in the VJISS network is for law enforcement purposes or justice purposes only and shall only be released or disseminated in accordance with these policies or policies associated with the operation of VLETS. Any use and dissemination of information in VJISS for personal or financial gain is strictly prohibited and may be subject to criminal prosecution (theft of services) and loss of access privileges for the user and agency.

#### 6. Enforcement

6.1 If a user is suspected or found not to be complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, or disclosure of information, the contributing agency or user agency will:

6.1.1 Suspend or discontinue access to information by the user.

6.1.2 Suspend, demote, transfer or terminate the person as permitted by applicable personnel policies.

6.1.3 Apply other sanctions or administrative actions as provided in agency personnel policies.

6.1.4 Refer the matter to appropriate authorities for criminal prosecution as necessary to effectuate the purposes of the policy.

I have read and understand the previous policies. Please Print this form, print your name

and sign in the boxes below and return to [dps.help@vermont.gov](mailto:dps.help@vermont.gov)

Print Name

Signature