Valcour CAD/RMS System Policies

User Agreement

I. Purpose

Valcour is a proprietary software solution, developed by CrossWind Technologies, (hereinafter "CrossWind") designed exclusively for legitimate law enforcement use. Valcour is designed to be used by multiple departments or agencies as a secure automated Computer Aided Dispatch, Records Management, and Mobile Computing system that gathers data for a variety of criminal justice purposes, including but not limited to, records of services rendered, incident/event information, information about persons involved in investigations, crimes reported, arrests, stolen and recovered property and crime data.

II. Definitions

2.1 Valcour Agency. A law enforcement agency using Valcour in a read-write capacity that has a federal ORI number and whose mission, purpose, or focus is the investigation or prosecution of criminal activity. Hereinafter "Agency."

2.2 Non-Contributing Agency. An agency that uses the system in a read-only capacity for law enforcement investigative purposes. Hereinafter "Agency."

2.3 Designated Contact. The Valcour Governance Board, with input from CrossWind, will designate up to three technical contacts (hereinafter "Designated Contacts") per Site who will be responsible for communicating with CrossWind Technical Support by telephone or e-mail.

2.4 Personal Identifying Information. Personally identifiable information is one or more pieces of information, when considered together, or combined with other information, identifies a unique individual.

2.5 Program Manager. A representative from an Agency, that is one of the Agency's employees, who communicates with the staff at the user Agency, and is the primary point of contact with the Designated Contacts.

2.6 User. A user is an individual authorized by an Agency head to have access to the information contained in the database(s) of the Valcour 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. All users must have background checks before they are given access to the Valcour data.

2.7 Agency approved device. A device that the agency has the ability to restrict access to Valcour/message switch via 2-factor authentication/device authentication.

III. Agency Policies

Each Agency shall make any requisite changes to their rules and regulations to accommodate and enforce the Valcour System Policies.

IV. Use Limitations

4.1 All data residing on the system is the property of the respective agencies participating. Any release of data MUST be done by, or with the express consent of, the primary investigating Agency (the ORI who originates the data).

4.2 Because the system allows for personal identifying information (person records without incident detail) within the system to be shared among ORIs, those portions of the data is accessible to all users but may only be released or disseminated ONLY for law enforcement purposes. Examples of such personal identifying information may include but is not limited to dates of birth, place of birth, address and phone number – but not incident specific detail.

4.3 Any information from the system released for any reason other than a legitimate law enforcement purpose may be subject to criminal or civil penalties.

V. Security

5.1 Only individuals who have signed a user agreement and who comply with the user agreement shall be permitted to access the system. User will be assigned a unique user login and shall create a password that complies with contemporary security standards.

5.2 Only agency-authorized devices using the approved Valcour Soft Token 2-factor authentication system are allowed to access Valcour.

5.3 Users shall not allow any device or software (including browsers or add-ons) to store their passwords for Valcour nor shall they share their passwords with any other person. Likewise, users shall not leave any device logged on to Valcour unattended or allow any non-law enforcement personnel to access a device that has an active Valcour login enabled.

5.4 Users shall not access Valcour from any public computer.

5.5 Each Agency shall make a reasonable effort to insure that all users comply with the user policy and shall immediately inform the Program Manager(s) of any breach or possible breach of security and/or any violations or potential violations of this policy.

5.6 Although reasonable efforts are taken to insure system security, absolute security cannot be guaranteed. Therefore, the following material should be stored on the Valcour network <u>at the user's discretion</u>:

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

B. Information which, if compromised, would place an individual in jeopardy – including but not limited to the names of confidential informants.

5.7 Users shall report any suspicious system activity to the Agency Program Manager.

5.8 Users shall not provide, discuss, or describe system related information of any kind with non-law enforcement personnel.

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

5.10 All logging of system activity is based on login and password. Login and password security is CRITICAL.

A. Users may be held responsible for anything that takes place utilizing their login. DO NOT REVEAL YOUR PASSWORD TO ANYONE FOR ANY REASON. Do not allow anyone to use your login and password. Valcour Program Managers will NEVER need to ask you for your password.

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

C. If you feel that the secrecy of your password has been compromised, change it immediately and notify your Agency Program Manager.

D. If you forget your password, send a request for password reset to the help desk (Valcourhelp@bpdvt.org). A new password will be securely transmitted to the user.

VI. System Usage

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

6.2 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, inaccurate, or inappropriate. Any user who modifies data inappropriately may be subject to sanctions contained below and/or to criminal prosecution.

VII. Policy Review

This policy shall be reviewed by Agency and/or Program Managers annually, or as required. Suggested policy changes must be approved by the Valcour Governance Board

VIII. Acknowledgements & Support

8.1 Program Managers reserve the right to monitor the system.
8.2 Program Managers may request changes to this document where it can be shown that such changes are needed in order to enhance security or operational capacity. Changes can be made subject to the Valcour Governance Board's approval.
8.3 Users shall report any problems, errors, or requests to the Valcour help group by sending email to Valcourhelp@bpdvt.org.
8.4 Users are encouraged to first contact an Expert User to try to resolve problems or questions. Users are encouraged to utilize all resources provided by their Agency, including experts users, online Help and the Agency Info page to troubleshoot prior to sending help desk requests.
8.5 Users shall notify a supervisor of any Valcour related issue that requires immediate attention. Supervisors shall follow the Valcour support flow chart to enlist assistance.
8.6 Users shall not attempt to change any system setting or perform any system modifications.
8.7 Occasionally the system will need to be brought down for maintenance. Advance notice will be given where practical.

IX. Sanctions

9.1 Agencies and users of the system shall adhere to this policy and any other mandatory rule, policy or procedure of the systems that co-exist with Valcour including but not limited to VIBRS network, the Vermont Justice Information Sharing System (VJISS) and NCIC - the FBI Criminal Justice Information Systems related policy. Failure to do so may result in the user or Agency being sanctioned.
9.2 Sanctions could result in a loss of privileges (disconnection) of the Agency or user and may be subject to civil and/or criminal liability and/or prosecution in state and/or federal court.
9.3 Sanctions may include the imposition emergency sanctions, including disconnection, if a security threat sufficient to warrant such action exists. Any disconnection will be subject to the review and concurrence of the Valcour Governance Board.

I hereby acknowledge receipt and understanding of the Valcour System Policies. I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which my agency authorizes me to engage. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information for a purpose other than that envisioned by my agency, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than that envisioned by my agency also constitutes misuse. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

______________________________ ______________ ________________
User Name User badge or ID # Date

______________________________ _________________________
User Signature Agency

____________________________________ ( ) User needs dispatching privileges
Supervisor Signature