Stowe Police Department

General Order: 1.26 **VT CJIS Advanced Authentication**	**Related General Orders:**
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.	
Applicable Vermont Statutes:	
Date Implemented: 06/18/2012	Date Revised:

I. PURPOSE:

1. The purpose of this policy is to establish the guidelines to help ensure that only authorized individuals gain access to CJIS systems via a variety of authentication methods in an effort to preserve the confidentiality, integrity, and availability of CJIS information as it is processed.

II. SCOPE:

1. The scope of this policy is to define appropriate and acceptable advanced authentication methodologies for use on the Stowe Police Department's computer system for accessing the CJIS systems and its associated data. Acceptable authentication is determined by the CSA based on the ability to support a particular methodology.

III. DEFINITION:

1. Advance authentication is achieved when a user presents, verified across the network, any combination of at least two of the following credentials:

- Something the user knows (e.g., password/pin)
- Something the user has (e.g., token, smart card or challenge card)
- Something the user is (e.g., a biometric such as a fingerprint or iris scan)

IV. POLICY:

1. Procurements and upgrades to systems, after 9/30/2005, that are part of or access

CJIS from any internet, wireless, or dial-in connection that is not physically secured shall use advanced authentication.

2. All mobile devices such as PDA's, cell phones transmitting CJIS data, and mobile data computers which have been removed from a police vehicle shall, at a minimum also incorporate the use of a unique password or other personal identifier (PIN) as well as meet the advanced authentication requirement.

3. Currently the only advanced authentication supported by the CSA is through the use of RSA Secure ID cards. This authentication utilizes a password to access the authentication system which then queries the user for a numeric identifier generated from an electronic token in the possession of the user. If this dual authentication is met then the user is granted access to the network. This authentication takes place across the network.

4. In order to receive access through secure ID the individual must have Stowe Police Department authorization and file the paperwork as required by the CSA, who will then make a determination as to the granting of access.

V. ENFORCEMENT:

CSA agency retains the right to terminate service in the event of a serious violation or failure to comply. Any violation of this policy may be grounds for disciplinary action consistent with any applicable collective bargaining agreement, statute, Department policy or Town policy.

Issued by:_____

Donald Hull
Chief of Police