Stowe Police Department

General Order: 1.25 **VT CJIS Acceptable Use**	**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. OVERVIEW:

1. The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to Stowe Police Department established culture of openness, trust, and integrity. The Department is committed to protecting Stowe Police Department employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, File Transfer Protocol, and National Crime Information Center access, are the property of the Stowe Police Department. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every Stowe Police employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

II. PURPOSE:

1. The purpose of this policy is to outline the acceptable use of computer equipment at the Stowe Police Department. These rules are in place to protect the employee and the Stowe Police Department. Inappropriate use exposes Stowe Police Department to risk including virus attacks, compromises of the network systems and services, and legal issues.

III. SCOPE:

1. This policy applies to employees, contractors, consultants, temporary staff, and

other workers at Stowe Police Department, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned or leased by the Stowe Police Department.

IV. POLICY:

GENERAL USE AND OWNERSHIP

1. While Stowe Police Department's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Stowe Police Department. Because of the need to protect Stowe Police Department's network, management cannot guarantee the confidentiality of information stored on any network devise belonging to the Stowe Police Department.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or management.

3. For security and network maintenance purposes, authorized individuals within the Department may monitor equipment, systems and network traffic at any time.

4. The Stowe Police Department reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

SECURITY AND PROPRIETARY INFORMATION

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

3. All personal computers, laptops, and workstations should be password-protected for security.

4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with "Mobile Data

Security Policy". General Order 1.30.

5. All devices used by employees that are connected to the Stowe Police Department Internet/Intranet/Extranet, whether owned by the employee or Stowe Police Department shall be continually executing approved virus-scanning software with a current database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

UNACCEPABLE USE

1. The following activities are, in general, prohibited. Under no circumstances is an employee of Stowe Police Department authorized to engage in any activity that is illegal under local, state, federal, or international law, or violation of Department or Town policy. The list below are by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

SYSTEM AND NETWORK ACTIVITIES

1. The following activities are strictly prohibited, with no exceptions:

    A. Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.).

    B. Installation of any copyrighted software for which Stowe Police Department or end user does not have an active license is strictly prohibited.

    C. Installation of any software without preapproval and virus scan is strictly prohibited.

    D. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).

    E. Revealing your account password to others or allowing use of your account by others.

    F. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, “disruption” includes, but is not limited to, network sniffing, packet floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

G. Port scanning or security scanning is expressly prohibited unless prior notification has been given the Chief of Police.

H. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

I. Circumventing user authentication or security of any host, network, or account.

J. Interfering with or denying service to any user other than the employee's host.

K. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

L. Providing information about NCIC or list of Department employees to parties outside the Stowe Police Department.

V. ENFORCEMENT:

1. Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action consistent with any applicable collective bargaining agreement, statute, Department policy or Town policy.

Issued by:_____

Donald Hull
Chief of Police