Stowe Police Department

General Order: 1.31 **VT CJIS Password Policy**	**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. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Stowe Police Department's entire network. As such, all Department employees (including contractors and vendors with access to the Stowe Police Department systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

II. POLICY:

1. All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

2. On all systems (procured after 9/30/2005) password reuse of the last ten (10) passwords shall be prevented if the password is used for authentication.

3. All production system-level passwords must be part of the Information Security administrated global password management database.

4. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed when prompted.

5. User accounts with access to NCIC privileges must have a unique password from all other accounts held by that user.

6. Passwords must not be inserted into email messages or other forms of electronic communication.

7. Where simple network management protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private, "and "system" and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

8. All user-level, system-level, and NCIC access level passwords must conform to the guidelines described below.

Password Construction Guidelines

1. Passwords are used for various purposes at the Stowe Police Department. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

A. Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - o Name of family, pets, friends, co-workers, fantasy characters, etc.
    - o Computer terms and names, commands, sites companies, hardware, software.
    - o The words "Stowe Police," "WVSP," "HPD," "CKSFP" or any derivation.
    - o Birthdays and other personal information such as addresses and phone numbers.
    - o Word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.
    - o Any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc.
    - o Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

2. Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+{}[]:";<>?,.?
- Are at least eight alphanumeric characters long.
- Are not words within any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
  NOTE: Do not use either of these examples as passwords

Password and Logon Deletion

1. All passwords and/or logons that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

2. When a password is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- Supervisor or POC should put the deletion information in writing and forward it to the Departments appropriate Technology Officer.
- The Departments Technology Officer will then delete the user's password and delete or suspend the user's account.
- The Technology Officer will forward confirmation to the Chief of Police that the password has been deleted and user account was deleted or suspended.

Password Protection Standards

1. Do not use your user id as your password. If you do not authenticate against DPS active directory do not use the same password for Stowe Police Department accounts as for NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share Stowe Police Department passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Stowe Police Department information.
Here is a list of "do not's"

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an mail message
- Don't reveal a password to the boss
- Don't talk about a password in front of others

- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with family members
- Don’t reveal a password to a co-worker while on vacation
- Don’t use the "Remember Password" feature of applications
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY computer system without encryption.
- Don’t reveal password to anyone for any reason!!!!

2. If someone demands a password, refer them to the Chief of Police or his/her designee.

3. If an account or password is suspected to have been compromised, report the incident to the Chief of Police or his/her designee and change all passwords.

4. Password cracking or guessing may be performed on a periodic or random basis by the FBI or individual or contractor authorized by the Chief of Police. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

1. Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other’s password.
- Should support Terminal Access Controller Access Control System+(TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

Remote Access Users

1. Access to the Stowe Police Department networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

III. ENFORCEMENT:

1. Discipline: 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