

Stowe Police Department

General Order: 1.27	Related General Orders:
VT CJIS Anti-Virus	
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. To establish requirements which must be met by all computers connected to Stowe Police Department networks to ensure effective virus detection and prevention.

II. SCOPE:

1. This policy applies to all Stowe Police Department computers that are PC-based or use PC-file directory sharing. This includes, but is not limited to, desktop computers, file/ftp/tftp/proxy servers, and any PC-based equipment.

III. POLICY:

1. All Stowe Police Department PC-based computers must have Department standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date.
Recommended processes to prevent virus problems:

- Always run the corporate standard.
- Run the current version and install anti-virus software updates as they become available.
- Anti-virus software is to be enabled on all workstations and servers at startup and employ resident and real time scanning.
- Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways.

- On servers, update virus signatures files immediately, or as soon as possible, with each new release.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk-sharing with read/write access unless there is absolutely an agency requirement to do so.
- Always scan a removable media from an unknown source for viruses before using it.
- Always scan any media that is brought into the agency before introducing it to the network.

2. Any activities with the intention to create and/or distribute malicious programs into Stowe Police Department’s networks (e.g., viruses, worms, Trojan horses logic bombs, etc.) are prohibited. Virus-infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on your workstation and the anti-virus software can not eliminate the virus, notify your supervisor. DO NOT TURN OFF your computer, it should be quarantined and should be taken off of the network until it can be scanned and re-imaged with the operating system image.

IV. 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