

# Stowe Police Department

<b>General Order:</b> 1.34	<b>Related General Orders:</b>
<b>User Account/Access Validation Policy</b>	
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.	
<b>Applicable Vermont Statutes:</b>	
Issued By: Donald B. Hull, Chief of Police	
Date Implemented: 08/01/2019	Date Revised:

## **I. POLICY:**

1. All accounts shall be reviewed at least every six months by the Terminal Agency Coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.
2. The Terminal Agency Coordinator (TAC) for the Stowe Police Department is: Officer Darron Tabor
3. All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.
4. The TAC must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)
5. The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual's account(s) to the new office (CJA).

6. The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.
7. Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC).
8. The TAC shall:
  - A. Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
  - B. Periodically review existing accounts for validity (at least once every 6 months), and
  - C. Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

## **II. DISCIPLINE:**

1. Any violation of this policy may be grounds for disciplinary action consistent with any applicable collective bargaining agreement, statute, Department policy or Town policy.