

STATE OF VERMONT Department of Public Safety VIBRS Network – Information Technology Policies		
Division: CJS Section: IT Policy Type: Department Wide Securing Unattended Workstations	ORIGINAL POLICY DATE: 7/31/07	ORIGINAL POLICY NUMBER 2007- 101
	EFFECTIVE DATE Upon Signature and distribution	IDENTIFIER

POLICY TITLE: Securing Unattended Workstations

POLICY STATEMENT: This policy requires all workstations utilizing the Vermont Incident Based Reporting System (VIBRS) network to be adequately secured when unattended, in order to protect the confidentiality, availability, and integrity of the Department of Public Safety’s information technology resources. Specifically this policy is intended to address the following VIBRS User Policy statement:

Users shall not leave a logged-in terminal or workstation unattended or unlocked.

POLICY DISTRIBUTION: After signature, to all DPS employees

PURPOSE: The purpose of this policy is to ensure the best practices of securing desktops is maintained in order to protect information contained in the Public Safety network by automatically locking terminals or workstations at after certain intervals of inactivity. The purpose of this policy is also to conform to the VIBRS User Policy, Section 9.6, Users shall not leave a logged-in terminal or workstation unattended or unlocked.

Applicability: This policy is to be adhered to by all employees of the Department of Public Safety and those agencies whose systems are managed through the active directory system administered by the Department of Public Safety.

1) General Standards

- a) Only authorized users are granted access to the VIBRS network and, thus, individual users are responsible for maintaining the security of their assigned workstation (PC, laptops, etc.). In order to prevent unauthorized system access, users must lock unattended workstations before leaving their work area. This shall be accomplished by manually invoking the screensaver (by striking the window key and the “L” key at the same time) when they leave their logged-in PC unattended (VIBRS User Policy Section 9.6).
- b) The Division of Criminal Justice Services information technology staff is responsible for establishing through the active directory system a password-protected screensaver after a maximum of ten (10) minutes of inactivity.

- c) Employees must not disable configuration specifications established by their department.
 - d) Anyone using access to the network through a securID token shall be locked out of the system after 4 hours of inactivity.
- 2) An exception to the automatic locking may be made by sending a request to the Director of the Division of Criminal Justice Services. The request should include a strong business case, supported by the person's chain of command, that the need to keep a system unlocked is based on a life safety issue.
- i) If a request is granted the person is still required to comply with the policy of not leaving a terminal, keyboard or workstation unattended or themselves by using the "windows, L" feature on their keyboard.

3) Enforcement

- a) Any employee found to have violated this policy may be subject to loss of privileges or other actions, up to and including termination of employment (See VIBRS User Agreement, and DOP policy 11-7)

Signature Section 2007-101

.....

Section Signature

10/30/07
DATE

Tom Davis
Tom Davis
IT Manager
Criminal Justice Services

.....

Division Signature

10/30/07
DATE

Francis (Paco) X. Aumand, III
Francis (Paco) X. Aumand, III
Director
Criminal Justice Services

.....