State of Vermont Agency of Human Services Department of Corrections	Title: Computer User Security Responsibilities	Page 1 of 3
Chapter: Management Information Systems	**#257.01**	**Supersedes:** # 257.01 dated 2/28/2000.
Attachments, Forms & Companion Documents: N/A		
Local Procedure(s) Required? No **Applicability**: All staff (including volunteers and contractors). **Security Level:"B"**- Anyone may have access to this document.		
Approved: **Andrew A. Pallito, Commissioner**	**September 11, 2012** **Date Signed**	**January 2, 2013** **Date Effective**

PURPOSE

The purpose of this administrative directive is to outline the access requirement for individuals using the Vermont Department of Corrections' (DOC) automated information systems.

This directive applies to anyone authorized to access information, to enter data, or to update non-public information on Department of Corrections' information systems.

POLICY

The intent of this administrative directive is to avoid unnecessary risk to the Agency of Human Services (AHS), users, and the individuals and families whom AHS serves; to improve productivity through efficient use of resources; to comply with applicable policies and law; and to minimize disruptions to services and activities.

AUTHORITY

28 V.S.A. 102(C) (1).

REFERENCE

22 V.S.A. § 901, 13 V.S.A. §§ 4101 through 4107, 28 V.S.A. § 102. State of Vermont *Physical Security for Computer Protection Policy*. State of Vermont *User Password Policy*. Agency of Human Services *Information Technology and Electronic Communications Policies*.

DEFINITIONS

Automated Information System (AIS): An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, and storage of information. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment. Management information systems are a common example of automated information systems. This assists in gathering information.

Designee: In instances where there is a foreseen absence, the IT Manager may assign another IT Staff member to perform duties as outlined in this directive.

Help Desk Ticket: A request for support from IT staff though completion of an online request system.

IT: Information Technology.

IT Local Administrator/Liaison: A Department of Corrections employee designated by the local manager at their local site, who has the responsibility for assigning computer access and/or network privileges to a DOC employee, a temporary employee, or a contractor at that site.

IT Staff: State of Vermont employees designated to support business functions by providing help desk, network, database, and other related IT services.

IT Manager: An Agency of Human Services employee designated as a liaison to a specific department within the Agency.

Network Privileges: The authorization given to users that enables them to access specific resources on the network such as email, data files, applications, printers, and scanners. Network privileges also designate the type of access; for example, can data only be viewed (read only) or can they be updated (read/write). Also called "user rights," "user authorizations," “user permissions,” and "user privileges."

PROCEDURAL GUIDELINES

1. Introduction

The Department of Corrections (DOC) maintains confidential information on its automated information systems. It is therefore required to protect those systems from unauthorized access and to maintain confidentiality and integrity of the systems and the data. Security is maintained by use of a username and password.

2. Physical Security

a. As outlined in the State of Vermont *Physical Security for Computer Protection Policy,* DOC computer workstations shall not be operated by anyone not having the authority to do so. Anyone observing such a violation shall report the incident to the local site IT Administrator/Liaison or the IT Manager.

b. Computers shall not be left unattended with the user logged into the system. During working hours, DOC staff will ensure computers are either turned off or locked when they are not in use. While it is not necessary to turn the units off overnight, users shall log off or lock computer workstations at the end of their workday.

c. No one other than IT staff shall connect or disconnect any device to the DOC computer network except under direction of IT staff.

d. No one other than IT staff shall install software on DOC computers except under direction of IT staff.

3. Information Technology Responsibilities

a. Facility Superintendents and District Managers will assign a designated staff member at their site as the IT local Administrator/Liaison, who is responsible to cover the following:

i. Ensure that staff members (including temporary employees and contractors) have read applicable State, Agency, and Department computer use information as listed in the Reference section of this directive prior to accessing DOC automated information systems.

ii. Make requests to IT staff for creation, transfer, and termination of DOC staff computer accounts by submitting a Help Desk ticket.

iii. Ensure that the staff members at their site are granted appropriate levels of network privileges to be applied by the IT staff.

b. The IT Manager or designee will facilitate all requests from IT local Administrators/Liaisons concerning this directive.

c. All staff members with access to a computer are responsible for reading applicable State, Agency, and Department computer use information as listed in the Reference section of this directive prior to accessing DOC automated information systems.

4. Username and Password Security

a. No person shall divulge their password to another person, nor shall any person use another's password, except when required in an emergency or in order to comply with instructions with IT staff. If there is any uncertainty as to the identity of the person requesting the password or the purpose for which it is requested, the individual shall not divulge their password. The password must be changed after the emergency or when service is completed.

b. All staff shall reference the State of Vermont *User Password Policy* for further guidelines on appropriate use and protection of usernames and passwords.

c. Any staff member with reason to believe that security has been breached shall report it to the IT Manager or designee immediately.

TRAINING

a. District Managers and Facility Superintendents, or their designees, will ensure that assigned local IT Administrators/Liaisons provide information to staff and/or how to access information, and answer any staff questions in relation to this directive.

b. The Deputy Commissioner will assign a Central Office staff member to be the local IT Administrator/Liaison who will provide information to staff and/or how to access information, and answer any staff questions in relation to this directive.

QUALITY ASSURANCE

IT staff may conduct periodic security audits as directed by Federal, State, or Agency mandates, policies, and guidelines.