

COMPUTER ACCESS

1. PURPOSE: To define policy, procedures, and responsibilities to effectively manage access to local Automated Information Systems (AIS).

2. POLICY: Access to any AIS will be granted on a need-to-know basis and authorized by the user's Service Chief or designee. Access will not be authorized on an individual's perceived need, position or precedence. Access requests to remote systems must be routed through the Information Security Officer (ISO) for review or processing.

3. PROCEDURES:

a. The ISO monitors the issuance and use of access codes to ensure:

(1) No person is granted access indiscriminately to any AIS containing sensitive information.

(2) Access to AIS is granted to employees on a need-to-know basis only.

(3) A signed security agreement is on file for employees having access to VistA, Wide Area Networks (WANs), Local Area Networks (LANs), or other remote sites.

(4) All terminated employees' accesses are immediately canceled upon separation from employment.

b. Information Systems Staff will:

(1) Upon e-mail notification of a new user, create an access code, and if applicable, PIN numbers, for all new users.

(2) Create LAN Network Accounts for new users as requested.

(3) Ensure all accounts of departing employees are properly deactivated in a timely manner.

c. Service or section level procedures:

(1) The Automated Data Package Application Coordinator (ADPAC) of each service or section will enter new users into the VistA "NEW PERSON," file and assign the appropriate menu options.

(2) The ADPAC will ensure the new user signs the security agreement, once received from the ISO, and is trained on log-on and log-off procedures as well as the utilization of the assigned menu options. All signed security agreements will be forwarded to the ISO (42).

(3) ADPACs must update the NEW PERSON file when a staff member is reassigned or transferred to another service within the VA Ann Arbor Healthcare System.

(4) Supervisors will ensure all terminating staff from their service out-process through the Information Systems Help Desk prior to the staff member's departure. Service chiefs will not sign off on the Clearance Form for Information Systems.

(5) Section chiefs or Human Resources will immediately notify the CIO/Information Systems staff if a staff member poses a potential threat to any system or is suspended or relieved of duties due to disciplinary action.

c. Employee's VistA privileges will be denied or terminated if:

(1) The employee poses a threat to VistA, or;

(2) the employee is suspended or relieved of duties resulting from disciplinary action.

d. Access codes will be issued by Information Systems staff or the ISO and the employee will be notified to pick up a sealed envelope marked "RESTRICTED to be opened only by *EMPLOYEE'S NAME*." ADPACs are not permitted to open these envelopes. Under no circumstances will an access code be issued via telephone.

e. Users are prompted to create their own verify code. Verify codes must be at least 6 characters in length and no greater than 20 characters. The code must include both alphabetic and numeric characters.

f. Users are required to change their verify code every 90 days; or if they believe their code has been compromised; or at the direction of the Information Systems staff or ISO.

g. Access codes for users at remote sites will be mailed to the remote site's ISO in a double sealed envelope. Under no circumstances will access codes be issued via the telephone system.

h. Inactive VistA accounts, 90 days or greater, will be deactivated. Users must contact the ISO or Information Systems Help Desk to reactivate their VistA account. This must be done in person.

i. Medical students, work-study students, work without compensation (WOC) employees, and temporary employees will be granted access to VistA with a predetermined termination date.

4. RESPONSIBILITIES:

a. The ISO will implement and monitor systems and safeguards to ensure VAAHS-wide compliance with the computer access policy.

b. Section Chiefs will ensure:

(1) The service ADPAC updates the NEW PERSON file when staff members transfer to another service within VAAAHS.

(2) The service ADPAC trains all new staff members on AIS security awareness prior to issuing the employee's access code.

c. Supervisors will ensure:

(1) Monitoring staff for possible breaches of security.

(2) New staff members attend New Employee Orientation within 30 days of their appointment.

d. Employees will safeguard their access/verify codes and protect sensitive information/data.

e. The Chief Information Officer and Information Systems Administrator will ensure Information Systems staff immediately terminate an employee's computer access prior to signing off on the Clearance Form.

5. REFERENCES:

VHA Directive 6210, Automated Information System (AIS) Security
Privacy Act of 1974 (Public Law 93-579)
The Computer Security Act of 1987, (Public Law 100-235)
JCAHO Comprehensive Accreditation Manual for Hospitals, Management of Information
chapter

6. RESCISSION: Policy Memorandum 40-2, dated September 19, 1997

7. EXPIRATION DATE: October 1, 2001.

8. FOLLOW-UP RESPONSIBILITY: Information Security Officer (42)



JAMES W. ROSEBOROUGH
Director

Distribution E