Effective Date: 6/28/2005
Revised Date:
Review Date:

North Sound Mental Health Administration

Section 4000 – Information Systems: Access Codes and Passwords

Authorizing Source:
Cancels:
See Also: Approved by: Executive Director Date: 6/28/2005
Responsible Staff: Motion #

POLICY #4002.00

SUBJECT: ACCESS CODES AND PASSWORDS

POLICY

NSMHA's mission and guiding ethical principal place great value on the privacy and confidentiality information. Beyond these principles, this privacy and security are mandated by state and federal laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These regulations require that NSMHA deploy and maintain a set of policies, practices, and technologies to safeguard confidential information and ensure that such information is not disclosed to anyone without the proper authorization to view or possess such information.

Access Codes and Passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

The IS/IT department will institute a system of access controls consisting first of a unique identification code and password requirement for each employee with a need to use NSMHA computer systems and network. The characteristics of the password requirement consist of the following:

1. The password must consist of at least 8 alphanumeric characters from at least three of the following:

    a. Upper case letters
    b. Lower case letters
    c. Numbers
    d. Special characters (*, #, &, etc.)

2. Each user must change the password every 30 days.

IS/IT Department Responsibilities

1. The IS/IT department shall be responsible for the administration of access controls to all company computer systems.
2. The IS/IT department will deploy and maintain a set of system/network access and password procedures that require unique user identification codes and passwords that conform to the characteristics outlined above.
3. The IS/IT department will maintain a list of administrative access codes and passwords and keep this list in a secure area.
4. Set the default to change passwords at least every 30 days.
5. Set the default so that passwords must consist of at least 8 alphanumeric characters from at least three of the following: Upper case; Lower case; Numbers; Special Characters.

6. Set the default to activate a password protected screensaver, set for 10 minutes.
7. Set the default that after three failed attempts to log on, the system will refuse to permit access for 30 minutes.
8. Set the default for a password history of 24 remembered passwords.
9. No less than annually, the IS/IT department will conduct an audit of the access code and password policy and practice. The results of this audit will be forwarded to the Privacy Officer.

Employee Responsibilities
Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. This should be strictly interpreted by all staff.
3. Passwords must be changed immediately if it is suspected that they may have become known to others. In the event that an employee suspects or knows that his/her password has become known to another person, the employee should immediately report this event to the IS/IT Department.
4. Passwords should not be recorded. This means practically that passwords should not be written on "sticky" notes on the monitor, placed on paper and taped to the bottom of the keyboard, etc.
5. Will change passwords at least every 30 days.
6. Should use passwords that will not be easily guessed by others.
7. Should lock their workstation when leaving their office.
8. Shutdown their workstation when leaving for the day.

Emergency Access to Applications/Files
An emergency may arise in which a user needs access to a system resource that is password-protected under another user ID and where that particular user is unavailable. In no circumstance should the original user ID-account owner's password be shared to access the application/files. In order to have a clear chain of responsibility, the IS Specialist will make available the application/file as needed and as able.

Managers' Responsibility
Managers should notify the IS/IT department promptly whenever an employee has provided notification that they are intending on leaving the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Enforcement
All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with NSMHA's Employee Conduct and Discipline policy.

ATTACHMENTS
None