

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

North Sound Mental Health Administration

Section 4000 – Information Systems: Remote Access

Authorizing Source:
Cancels:
See Also:
Responsible Staff: IS Specialist

Approved by: Executive Director
Motion #:

Date: 6/28/2005

POLICY #4010.00

SUBJECT: REMOTE ACCESS

POLICY

Remote access is a generic term used to describe the accessing of the computer network by individuals not located at the organization's primary office. This may take the form of traveling employees, employees who regularly work from home, or employees who work both from the office and from home. In many cases, both NSMHA and the employee may benefit from the increased flexibility provided by a remote access program. As with any innovation, however, the benefits may be countered by risks if the purposes and methods of the program are not fully understood by all participants.

To optimize the efficiency of our remote access program, we have created a clear policy governing eligibility, obligations and responsibilities of remote users.

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting NSMHA needs. The Agency may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

NSMHA procedures for remote access are as follows:

A. Acceptable Use

Hardware devices, software programs, and network systems purchased and provided by NSMHA for remote access are to be used only for creating, researching, and processing NSMHA-related materials. By using NSMHA hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable policies, as well as City, State and Federal laws and regulations.

B. Equipment & Tools

NSMHA will provide some of the tools and equipment for remotely accessing the corporate computer network in a secure manner. This may include computer hardware, software, e-mail (does not include Outlook Web Access), voicemail, VPN configuration, connectivity to host applications, and other applicable equipment as deemed necessary.

Remote access via dial-up modem will not be permitted except for emergency system administration access by the IS/IT Department. Broadband connections are required for remote access. Users are responsible for establishing working broadband connections in their own homes and ensuring there is a network connection available to connect NSMHA equipment.

The use of equipment and software for remotely accessing the computer network is limited to authorized persons and for purposes relating to NSMHA business. NSMHA will provide for

repairs to NSMHA equipment. NSMHA employees may not use their own personal computers to remotely access NSMHA internal network.

C. Password and Privacy Protection

By using NSMHA hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with NSMHA Access Code and Password policy. In addition, the employee agrees to take maximum precautions to prevent unauthorized access and/or viewing of client's protected health information during remote access sessions. To do this, employees must agree to place the computer in a secure environment (not in open living rooms or other common spaces) and lock the workstation when briefly leaving the computer. Additionally, employees will logoff of the NSMHA network when absent from the computer for extended periods.

D. Enforcement

Penalties for violation of the Remote Access Procedure will vary depending on the nature and severity of the specific violation. Any employee who violates the Remote Access Policy will be subject to discipline up to and including termination from employment in accordance with NSMHA's Employee Conduct and Discipline policy.

ATTACHMENTS

None