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

North Sound Mental Health Administration

Section 4000 – Information Systems: Workstation/Laptop Acceptable Use

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

POLICY #4013.00

SUBJECT: WORKSTATION/LAPTOP ACCEPTABLE USE

OVERVIEW

The IS/IT Department is committed to protecting NSMHA's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of NSMHA. These systems are to be used for business purposes in serving the interests of NSMHA, and of our clients in the course of normal operations.

Effective security is a team effort involving the participation and support of every NSMHA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at NSMHA. These rules are in place to protect the employee and NSMHA. Inappropriate use exposes NSMHA to risks including virus attacks, compromise of network systems and services, and legal issues.

SCOPE

This policy applies to NSMHA employees, contractors, temporaries, and other workers at NSMHA, who have been granted logon rights to the NSMHA internal network. This policy applies to all equipment that is owned or leased by NSMHA.

POLICY

A. General Use and Ownership

1. While NSMHA's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of NSMHA. Because of the need to protect NSMHA's network, management cannot guarantee the confidentiality of information stored on any network device belonging to NSMHA.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.
3. IS/IT Department recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on encrypting email and documents, see NSMHA's Acceptable Encryption Policy.

4. For security and network maintenance purposes, authorized individuals within NSMHA may monitor equipment, systems and network traffic at any time.
5. North Sound Mental Health Administration reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

B. Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by the NSMHA Designated Record Set Policy, whether the information is Protected Health Information, or other information, which is privileged. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All PCs, laptops and workstations are configured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended.
4. Use encryption of information in compliance with NSMHA's Acceptable Encryption Policy.
5. Postings by employees from a North Sound Mental Health Administration email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of North Sound Mental Health Administration, unless posting is in the course of business duties.
6. All workstations or laptops used by the employee that are connected to the North Sound Mental Health Administration Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database.
7. Employees must use extreme caution when clicking on links in email messages or opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

C. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., IS/IT staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of North Sound Mental Health Administration authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing North Sound Mental Health Administration-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

D. System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NSMHA.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NSMHA does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. IS/IT Department should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

    a. The only exception to this is when IS/IT Department staff needs to temporarily elevate user privileges for the purpose of installing profile-specific software.
    b. This exception is only specific to the use of your account by another. You shall never reveal your account password. IS/IT Department staff will temporarily reassign your password and, when work is complete, will reset your password so that you may maintain the secrecy of your password.

6. Using a NSMHA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any NSMHA account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited except as those processes identified in the NSMHA Audit Vulnerability Scan Policy.
11. Executing any form of network monitoring which will intercept data not intended for the employee' host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Connecting any non-NSMHA peripherals (keyboards, printers, modems, etc.).

E. Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

PORTABLE COMPUTER

Employees, contractors, and others using portable computers (users) must read, understand, and comply with this policy.

Any portable equipment requested must be logged in the IS/IT Hardware Database. The hardware, software, all related components, and data are the property of NSMHA and must be safeguarded and be returned upon request and upon termination of your employment. You are responsible for the equipment NSMHA issue's you during your employment.

The user agrees to use the equipment solely for NSMHA business purposes. The user further understands:

1. Dial-up networking functions are only to be established by the IS/IT Department and configuration settings must not be altered by the user. User is not permitted to dial into any other unauthorized services, Internet service providers, or any other Internet access or to use the dial-up capabilities in any other manner than as instructed. The user understands that the hardware has been disabled from performing any functions other than those intended for business use and that the user may not attempt to enable such other functions.
2. Computers, associated equipment, and software are for business use only, not for the personal use of the user or any other person or entity.
3. Users will not download any software onto the computer except as loaded by authorized staff of the IS/IT Department.
4. Users must use only batteries and power cables provided by NSMHA and may not, for example, use their car's adaptor power sources.
5. Users will not connect any non-NSMHA peripherals (keyboards, printers, modems, etc.).
6. Users are responsible for securing the unit, all associated equipment, and all data, within their homes, cars, and other locations while checked out to the user.
7. Users may not leave mobile computer units unattended unless they are in a secured location.
8. Users should not leave mobile computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.
9. Users must securely place portable computers and associated equipment in their proper carrying cases when transporting them.
10. Users must not alter the serial numbers and asset numbers of the equipment in any way.
11. Users will not permit anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, clients, client families, or unauthorized officers, employees, and agents of NSMHA.
12. Users must not share their passwords with any other person and must safeguard their passwords and may not write them down so that an unauthorized person can obtain them. (See the Access Code and Password Policy).
13. Users must report in writing any breach of password security immediately to the IS Specialist, who in turn will notify the Privacy Officer.

14. Users must maintain confidentiality when using the computers. The screen must be protected from viewing by unauthorized personnel when confidential information is displayed, and users must properly log out and turn off the computer when it is not in use.
15. Users must immediately report in writing any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the IS Specialist, who in turn will notify the Privacy Officer.

A. 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