



DEPARTMENT OF THE NAVY
NAVAL MEDICAL RESEARCH CENTER DETACHMENT

LIMA, PERU
UNIT NUMBER 3800
APO AA 34041 - 3800

IN REPLY REFER TO

NMRCINST 5239.1E
29 October 2003

NMRC INSTRUCTION 5239.1E

From: Officer-in-Charge, Naval Medical Research Institute Detachment

Subj: AUTOMATED INFORMATION SYSTEM (AIS) SECURITY PROGRAM

Ref: (a) SECNAVINST 5239.3 Series
(b) OPNAVINST 5239.1B Series

Encl: (1) Network Security Officer (NSO) Responsibilities
(2) Terminal Area Security Officer (TASO) Responsibilities
(3) Information System User Responsibilities
(4) Information Systems Standard Operating Procedure (SOP)
& NMRC AIS Usage Policy and Network Security Policy

1. Purpose.

a. To establish network security policies and Automated Information System (AIS) assets and resources usage policies.

b. To prevent and detect abuse or misuse of AIS facility assets or resources by delegating responsibilities to identified personnel that will provide guidance to users on policies established.

c. To instruct personnel to preserve data from loss in case of damage to any AIS asset; and to protect NMRC data against alteration or unlawful use.

d. To establish NMRC voice and data communications operations and capabilities and assign responsibilities.

2. Cancellation. NMRCINST 5239.1D

3. Scope.

a. This instruction applies throughout the command with regard to network security policies and AIS assets and resources usage policies.

b. References (a) and (b) are the instructions which form the basis for AIS security within the Navy.

c. Enclosures (1), through (3) assigns responsibilities; enclosure (4) lists procedures to follow, defines the network security policies and AIS assets usage policies.

NMRCDINST 5239.1E
29 October 2003

4. Applicability. The term "Automated Information Systems" as used in this instruction applies to all Information System resources in use at NMRCD. These resources include all computer assets (desktop computers, laptop computers, peripherals, data collector systems, telephones, mobile phones, radios and pocket PCs) whether government or privately owned, in use to support NMRCD's mission.

5. Action. All AIS users, and their supervisors, are responsible to ensure compliance with all relevant instructions, and that any additional steps required to protect Command AIS resources are brought to the attention of the Network Security Officer (NSO). Duties of individuals within the AIS Security chain-of-command are delineated in the enclosures. These positions may be combined upon the discretion of the AIS Network Security Officer, if the number of workstations and customers within the organizational unit do not warrant additional support.

A handwritten signature in black ink, appearing to read 'J. K. Baird'. The signature is fluid and cursive, with a large loop at the end.

J. K. BAIRD

Duties and Responsibilities of the
Network Security Officer (NSO)

1. The NSO is responsible to the Officer-in-Charge to ensure that:
 - a. All Command AIS resources on the network are protected to the maximum level that available budget and technology permits. AIS resources include: AIS hardware, Data, Human Resources, Software, and Communications Capabilities.
 - b. All personnel comply with the relevant instructions, directives, and procedures concerning AIS procurement and security.

2. NSO duties directly bearing upon the responsibilities assigned above will include, but not be limited to:
 - a. Ensure that the level of security available on the network is sufficient to adequately protect data on the network.
 - b. Ensure that SOPs and training accurately inform the AIS Security chain-of-command and AIS users about security issues relevant to the network.
 - c. Ensure that all requirements concerning protection of equipment and data that are on the network are complied with. Special attention will be given to maintenance of maximum practical network reliability and protection against loss of data.
 - d. Ensure that unauthorized use and penetration of the network is prevented as much as is practical.
 - e. Develop, implement, and maintain the AIS security policies and guidance for NMRCD network.

Duties and Responsibilities of the
Terminal Area Security Officer (TASO)

1. The TASO is responsible to their Department Head and the Network Security Officer (NSO) to ensure that:
 - a. All Command AIS resources within their area of jurisdiction are used by personnel following the policies outlined in this instruction.
 - b. All relevant instructions, directives, and procedures concerning AIS procurement and security are complied with by all personnel.

2. TASO duties directly bearing upon the responsibilities assigned above will include, but not be limited to:
 - a. Maintain a detailed knowledge of all NMRCDC AIS instructions and policies.
 - b. Maintain a detailed knowledge of AIS activity, and data security levels within their area of jurisdiction.
 - c. Ensure that all personnel within their area of jurisdiction are sufficiently indoctrinated in AIS security to protect Command AIS resources.
 - d. Assist the NSO in testing, inspecting and evaluating AIS security procedures and plans within their department.
 - e. Investigate incidents and situations that may result in AIS security breaches and deficiencies. Reporting the results of these investigations to the NSO.
 - f. Ensure that access to Command AIS equipment and systems is only granted to appropriate personnel.
 - g. Ensure that AIS Standard Operating Procedures (SOPs) are followed by all personnel.

Duties and Responsibilities of the AIS User

1. The AIS User is responsible to their AIS security chain-of-command to ensure that:
 - a. All Command AIS resources under their care are protected to the maximum level practical following the policies outlined in this instruction.
 - b. All relevant instructions, directives, and procedures concerning AIS procurement and security are complied with.
2. AIS User's duties directly bearing upon the responsibilities assigned above will include, but not be limited to:
 - a. Maintain a detailed understanding of, and compliance with, all NMRCD AIS security instructions and policies.
 - b. Maintain a continued awareness of the security implications of the AIS systems and data that they use.
 - c. Take continual care to ensure that sensitive information is protected at all times.
 - d. Attend appropriate AIS security briefs and training.
 - e. Ensure that access to Command AIS equipment and systems is only granted to appropriate personnel.
 - f. Follow AIS Standard Operating Procedures (SOPs).
 - g. Report all incidents and conditions that may impact the Command's AIS security posture to their TASO or the NSO. This includes keeping the TASO fully aware of the sensitivity and type of all information processed on NMRCD equipment.

Automated Information Systems (AIS)
Standard Operating Procedures (SOP)
Network Security Policy
AIS Resources Usage Policy

Enclosure (4)

Introduction

The Naval Medical Research Center Detachment is the custodian of several million dollars worth of the Navy's Automated Information System Hardware, and millions more in data resources and software development time. The Department of the Navy (DON) Automated Information System (AIS) Security Program has been tasked to minimize the risks of loss, provide the maximum practical level of protection of AIS resources, which are defined as: hardware, data, human resources, software, and communications capability.

This Standard Operating Procedure (SOP) is Command policy and is intended as a day-to-day guide for AIS users at the Naval Medical Research Center Detachment. It is the duty of each user to ensure compliance, and the updating of this procedure to improve effectiveness when necessary.

Scope

This SOP applies to all AIS operations at, or sponsored by, NMRCD. Privately owned computer equipment used at NMRCD, or processing NMRCD data is covered by this SOP. NMRCD purchased equipment taken into the field, or used at detachments, is also covered.

Computers and Peripherals Policies

Computers and Peripherals Access

- All NMRCD employees with a network account are allowed to use the computers. This includes Foreign Service Nationals (FSNs), authorized contractors, and personnel with contract.
- Visitors only with the Administrative Officer (AO) and/or the Officer-In-Charge (OIC) approval.
- Visitors using the library, are to follow the Research Support's procedures. Currently we have 1 computer in the library for visitors and 6 in the Visitors Room.

NMRCD Policy for access to computers by visitors

- When authorized to visitor is allowed to use a computer, they are only the GUEST account. Information Systems Division (ISD) personnel will provide authorized visitors the access to use the GUEST account.
- AO or OIC can request a personalized account for a visitor staying in NMRCD for an extended period of time.
- DO NOT PROVIDE YOUR PASSWORD TO ANY VISITOR.

SCREEN SAVER POLICY AND LOCKING COMPUTERS

When you leave your work area for a period of time, any user is able to access all the information and resources you are allowed to if you do not log off from the network or protect your computer from being used while you are away. Screen saver and locking computers are methods to protect your computer from being accessed. For Windows 2000, XP and NT, is mandatory to lock computers while away from desk (by CTRL-ALT-DEL). For Windows 98, 95 or Millennium, use screen savers.

For screen savers, follow these recommendations:

- Some downloaded screen savers cause conflicts with other programs, causing computers to crash, therefore, only screen savers provided within Windows are allowed.
- It is mandatory to set a password for screen savers. Five minutes after inactive is recommended.
- It is recommended to change your screen saver password periodically.
- ISD will provide all support required to allow you to comply with NMRCD screen savers policy.

Turning computers off

- It is mandatory to turn off your computers at COB every day for the following reasons:
 - Energy saving
 - Security policy
 - Hardware protection - hard disk over heat when they are not turned of for a long period of time.

Off-site Computing Policy

NMRCD owned data may be removed from the Command for processing by permission of the TASO, NSO or the OIC as long as it is not sensitive or Privacy Act information. Sensitive and Privacy Act information may only be removed from the Command by permission of the OIC.

Ownership of Data

All information created or used on a Government-owned computer, or on personally owned computer operating on behalf of the Federal Government, is the property of the Federal Government. This information constitutes official records and is subject to all Federal statutes and regulations, such as the Federal Records Act, Privacy Act, Freedom of

Information Act, agency disposition schedules, etc., and must be adequately protected.

Protection of Data from Loss

- NMRCDC data is an extremely valuable part of the Command's AIS resources. Thus it is incumbent upon the users to ensure that all data is protected from loss or corruption. In fact, users that negligently lose or damage NMRCDC owned data are as culpable as people that lose or damage equipment.
- All users are required to store all important and valuable data on the server storage space assigned to each department and/or to each user. All data on servers are backed up on daily bases on tapes and several copies are stored on and off site.
- Any data stored in local hard drives are responsibility of each user. Proper local backup should be performed to ensure no data is lost.

Copyright Policy

- The DON and NMRCDC strongly denounce the violation of software copyrights. This is sometimes called "Software Piracy" and occurs when software is copied or used in violation of the license agreement issued with the software. Individuals found in violation of copyright agreement are subject to criminal prosecution under federal law.
- No program shall be installed on any computer without ISD authorization.
- Public Domain Software (and Shareware) is often readily available from bulletin boards and other sources. It is DON policy that such sources of supply must be considered suspect and possibly contaminated with "Viruses" or "Worms". These contaminations are segments of code deliberately designed to covertly enter a system and then perform varying levels of damage, to totally destroying the data and operating system. Some attacks have insidiously corrupted programming or data to cause initially undetectable damage. Public Domain software that is not obtained from an extremely reliable source will not be used on AISs covered by this SOP. Only ISD personnel are authorized to install software on computers.

Network Security Policies

Network Data Storage

Storage is provided for software and data that is intended to be used by more than one user, or from more than one workstation. The wasting of network storage requires the purchase of additional expensive hardware and deprives those with legitimate uses for the net of prompt service; thus, users must observe adequate criteria to decide what to save on the network and what not.

Passwords

DOD requires that all access to AIS resources be restricted to authorized personnel only. To accomplish this, passwords should be assigned to access the network and PCs. Once a password is assigned, it must be protected. This means that distribution is limited to only those authorized to use it. Individual user's network password should not be distributed to anyone else. Permissions over files, databases, Internet access, E-mail access is assigned to users. The password is the way to assure that nobody can use your assigned permissions to those resources.

NMRCD policy is:

- Password is SECRET. Nobody should know your password but you.
- If for some reason you provide your password to somebody, you should IMMEDIATELY change it.
- Changing password periodically is the best procedure to keep your password secret.
- Administrators are not able to see your password, but are able to change it for you in case you forget it or is compromised somehow.
- Changing your network password is mandatory. **60 days** is the limit for password change.
- ISD will provide all support required to allow complying with NMRCD password policy.
- The last five passwords cannot be repeated.
- The minimum length for a password is 6 and the maximum is 15.
- It is recommended to use a combination of numbers, characters and symbols for a password.
- It is not recommended to use easy-to-guess words like your name or a relative's name as password.

Network Account

Network Account is a set of credentials (Username and Password) that provides access to an entire network or a portion of it depending on the settings from the network administrator.

Procedure to Request a Network Account

1. The Department Head will send the request by E-mail to the NSO. The request must include the full name of the user and the period of time (if available) that the account will be active. It should also include if the account will have an E-mail address associated.
2. ISD will create the account and configure the access in the computer assigned to the end-user.
3. ISD will grant access to the files of the department that the user works for.

Username policy

The username is assigned by ISD using the following criteria:

1. For American Officers, username will be the last name.
2. For other users, username will also be the last name.
3. In case a username already exists, the first letter of the name will be added to the username as a prefix.
4. In case last name cannot be applied, ISD will decide a suitable username.

E-mail Account creation

When a network account is requested, it is usually requested with an E-mail account. If this is the case:

1. ISD creates an E-mail mailbox using the following E-mail address creation rules:
 - For American Officers, the address is the last name followed by @nmrcd.med.navy.mil
 - For other employees, the address is the first letter of the name followed by the last name and @nmrcd.med.navy.mil
 - If any of the above can be applied, ISD decides the best E-mail address to be applied.
2. Space limit is applied to every mailbox to avoid lack of hard disk space.
 - For American Officers, there is no limit.
 - For FSNS, "warning" is set to 8 MB and "prohibit

- to send* is set to 10 MB
 - For other employees, *warning* is set to 5 MB and *prohibit to send* is set to 6 MB
3. Because of the space limit, we setup *Personal Folders* to all users. It is users responsibility to maintain their personal folders on a suitable capacity. Over 2GB personal folders will fail to work and data will be lost.

E-mail Usage policy

- Use your E-mail only for work-related matters.
- Delete E-mails that are not in use anymore or store them in personal folders to reduce the use of disk space on the server.
- Do not subscribe to any list with NMRC D E-mail address unless it is a work-related matter.
- Follow instructions on virus warning messages that ISD issues periodically.
- We recommend sending E-mails with attachments smaller than 4 MB. Large attachments take long time to be sent. Other messages are kept in queues until the ones with large attachments are sent.

Recommendations to avoid infection with electronic Virus

- Do not open attachment with extensions like: vbs, pif, scr, com, exe.
- If you receive E-mail from unknown sender or subject, do not open it and communicate it to NSO or ISD department as soon as possible.
- Always verify that your Antivirus software is running (real-time) and is up to date. Do not turn the anti-virus program off.

Environment Controls

Electrical Power

All AIS equipment will use stabilized power. AIS equipment that is left in operation unattended, especially after working hours and on weekends, should be reported to the TASCO and the NSO.

Temperature/Humidity

The vast majority of AIS equipment at NMRCDC operates in an "office" environment. If it is safe for people, it is safe for the equipment. Specific guidance for each piece of equipment is included with its operating specifications. Each user must be aware of their equipment's limitations, and secure the equipment when conditions dictate.

Magnetic media, such as floppy disks and tapes, are very vulnerable to temperature and extreme humidity. Temperature ranges from 50 to 125 Degrees F. (10 to 52 Degrees C.) are often cited as safe operating limits.

Smoking

Cigarette, cigar, and pipe smoke produce massive contamination of the air. These contaminants coat magnetic media and read/write heads, causing hardware failure and loss of data. Smoking in the vicinity of AIS equipment and storage media is prohibited.

Handling of Media

As mentioned above, magnetic media is vulnerable to extremes of temperature and humidity. In addition mechanical protection must be provided to ensure data integrity. 3.5" Floppy disks, 100 and 250 MB zip disks, and CDs, must be protected from bending and crushing. Write on these disks only with a felt tip pen, as a ballpoint or pencil will damage the magnetic surface within. All magnetic media must be protected from exposure to magnetic fields. Holding your disk to the side of your machine with magnetic fields. Holding your disk to the side of your machine with a magnet is a good way to lose data. Dirt on the media will cause degradation and data loss; even fingerprints will cause damage. Keep the disks in their jackets whenever they are not in the drive.

Physical Protection

Water is the most probable environmental source of damage of AIS equipment. Sources of water damage can include: leaky roofs, plumbing/heating system failures, and drinks belonging to the user or others. The following rules will reduce the chances of water and dust damage:

- When possible, locate equipment in areas with no piping in the overhead.
- Keep food and drink away from the equipment.

Fire is a threat to all electrical equipment. The following rules will reduce the threat of fire, and the damage it may cause:

- Ensure that all AIS equipment is properly ventilated. Ensure that vent holes are not blocked and covers are removed when the equipment is energized.

AIS equipment is valuable and often easy to carry away. All personnel are responsible to ensure that all equipment that is in an area susceptible to unauthorized entrance is provided with some measure of protection. Inexpensive locks down devices are available to make it difficult to quickly remove this equipment. Common sense and good judgment must prevail.

Emergency Procedures

General

No piece of equipment or data is more valuable than a human life. All emergency responses must take place with the protection of the personnel involved given top priority.

These directions supplement and do not void existing command emergency bills.

Fire

1. Secure power to the equipment. Remove the power cord from the wall socket if possible. Be aware of any UPS that may continue supplying power when the building power is removed. Warning: damaged internal circuit may energize the exterior chassis of the equipment. DO NOT TOUCH UNTIL POWER IS SECURED.

If de-energizing the equipment does not extinguish the fire, use fire fighting agents. Agents are listed in order of decreasing preference:

Halon
CO2
Dry Chemical
Fresh Water

When the fire is extinguished, and the safety of personnel can be assured, tip equipment to allow drainage of any excess water or chemical. Notify cognizant personnel listed on the safety instruction.

Flooding

1. Secure power to the equipment. Remove the power cord from the wall socket if possible. Be aware of any UPS that may continue supplying power when the building power is removed. Warning: damage internal circuitry may energize the exterior chassis of the equipment. DO NOT TOUCH UNTIL POWER IS SECURED.
2. Remove equipment if possible to an area safe from flooding.
3. Tip equipment to allow drainage.
4. Notify cognizant personnel listed on the safety instruction.

Power Failures

If at all possible, power to AIS equipment should be secured in the event that problems with electrical power can be foreseen. If power fails, disconnect the equipment from the outlet and wait until the power is re-established and back to normal operation to re-connect it and turn the equipment on again.