



Branch Dental Clinic
Information Systems
Security Manager
Guide

December 1998

Table of Contents

<i>What is Information System Security Management?</i>	<i>ii</i>
<i>Applicable Instructions</i>	<i>ii</i>
<i>Information Security Philosophy</i>	<i>ii</i>
<i>Clinic Responsibilities</i>	<i>iii</i>
Training	<i>iii</i>
Monitoring Computer Areas	<i>iii</i>
Computer Access List	<i>iii</i>
Equipment And Media Labeling	<i>iii</i>
Information Security Levels	<i>iv</i>
Hardware and Software Inventory	<i>iv</i>
Authorized Software	<i>iv</i>
Reporting Security Problems	<i>v</i>
Reporting Changes	<i>v</i>
Clinic Information Security File	<i>v</i>
<i>Sample Forms</i>	<i>vi</i>
Computer Authorized User List	<i>vi</i>
Security Incident Report	<i>vi</i>
Information Systems Security Rules	<i>vi</i>

INTRODUCTION

Welcome to the Naval Dental Center Southwest Information Systems Security Management Team. As a Clinic Information Systems Security Manager (CISSM) you are a key element in our information systems security program.

Please read this booklet carefully. It contains important information for implementing information systems security in your area. All forms included in this booklet should be reproduced as needed. Realizing that this assignment is a collateral duty and represents only a portion of your actual duty, we have designed this booklet to identify your information systems security duties and to assist you in accomplishing these duties.

Please contact the Management Information Department (MID) at phone number 619-556-9143 (DSN 526-9143) for assistance or any additional guidance you may need.

What is Information System Security Management?

Information Systems Security Management (ISSM) is security for all resources related to information processing on computers. This includes the computer equipment, storage media, supplies, software, and data. Specifically, this means the computer, printer, video terminal, keyboard, other peripherals, floppy disks, tapes, paper, ribbons, computer programs, and information.

Applicable Instructions

SECNAVINST 5239.2	DEPARTMENT OF THE NAVY (DON) AIS SECURITY PROGRAM
OPNAVINST 5239.1A CH-1	DON AIS SECURITY PROGRAM
BUMEDINST 5239.1	BUMED AIS SECURITY PROGRAM
NDCSDIEGOINST 5239.1D	NAVDENCEN SOUTHWEST AIS SECURITY PROGRAM

Information Security Philosophy

Our philosophy is to provide employees and customers with the knowledge and tools required in managing one of our most valuable assets in a secure manner. This asset is information. Our goal is to provide a continuous security program encouraging all computer systems users to incorporate sound security practice into their everyday work habits.

Clinic Responsibilities

The Clinic Information System Security Manager (ISSM) is responsible for implementation and monitoring of microcomputer security requirements for their assigned area. Implement and ensure that users adhere to proper operational and security related procedures.

Training

Training is an important part of any security program. Clinic ISSM shall be trained by the Management Information Department (MID). Users shall be trained by clinic ISSM. Guides have be developed by MID to facilitate training. All users must sign a sheet acknowledging information has been passed and they will act within information security rules.

Monitoring Computer Areas

Clinic ISSMs should monitor the computer area during duty hours and prior to close of business to ensure that terminals are not left logged on and unattended. Users will follow proper security procedures.

Computer Access List

Clinic ISSMs should maintain a current list of all staff members who are authorized users of computers in their areas. The Computer Access List form in this booklet should be filled out and copies distributed as follows:

- (1) Original posted on or near Computer
- (2) Copy retained in Clinic Information Security file
- (3) Copy to Information Systems Security Manager in the MID Department.

Equipment And Media Labeling

Clinic ISSMs should ensure that computers and terminals are labeled as to the highest classification of data authorized for processing. Since CLASSIFIED information is prohibited on all machines, the highest classification will be either SENSITIVE UNCLASSIFIED. Labels are available from MID.

Clinic ISSMs must also ensure that users label all storage media, diskettes and tapes, as to the classification of the information contained. This classification will also be either SENSITIVE UNCLASSIFIED. Labels are available from MID.

Information Security Levels

CLASSIFIED - Classified information will **NOT** be input to, processed by, or output from any Naval Dental Center Southwest claimancy computer equipment. Classified information is information in any of the following security levels:

- (1) SCI
- (2) SIOP-SCI
- (3) TOP SECRET
- (4) SECRET
- (5) CONFIDENTIAL

The following levels of data may be processed on command computers, but measures must be taken to protect the information from unauthorized disclosure.

- (1) SENSITIVE UNCLASSIFIED DATA - Unclassified information requires special protection under federal law or by the nature of the subject matter.
- (2) PRIVACY ACT DATA
- (3) SENSITIVE BUSINESS DATA
- (4) FOR OFFICIAL USE ONLY
- (5) FINANCIAL
- (6) MEDICAL HISTORY
- (7) PRIVILEGED
- (8) EMPLOYMENT HISTORY
- (9) UNCLASSIFIED DATA - Non-sensitive data requiring normal protection.

Hardware and Software Inventory

Periodically you will be asked to validate hardware and software inventory for your area. You may be asked to provide a list of equipment with serial numbers, but usually you will be provided with an inventory list and asked to check it against the actual equipment and software in your area. Please annotate any discrepancies on the list and then sign and return it to MID.

Authorized Software

Most commercially available software is copyrighted by the company which develops and markets it. For a purchase price the purchaser buys the right to use the software in accordance with a license agreement which is specified by the company. Although provisions of license agreements vary from company to company and from product to product, most prohibit use of software on more than one computer.

To ensure that copyright laws are not violated, to prevent technical problems from viruses and software incompatibility, and to provide standardization of microcomputers within the

command, restrictions are placed on acquisition and loading of software. The Management Information Department is tasked with ordering and loading of all software. If software is needed in your area, contact MID to make arrangements for its procurement.

Make sure that your users do **NOT**:

- (1) make unauthorized or illegal copies of government owned software
- (2) bring in software from home
- (3) load any software without approval from MID.

Reporting Security Problems

All Information Security problems should be reported as soon as they occur or are discovered.

All of the following are reportable:

- (1) Incidents of vandalism
- (2) improper use
- (3) unauthorized disclosure
- (4) theft
- (5) accident
- (6) viruses

and should be reported to the Information Systems Security Manager for the system involved. A telephone report should be followed with a written report using the Information Security Incident Report form provided in this booklet.

Reporting Changes

When a Clinic ISSM leaves, a new one must be appointed in writing. Please notify the MID so that there will be no lapse in assignment.

If you need to move computer equipment within your area, please advise your clinic ADP Technician. This technician is trained to relocate your equipment with minimum chance for damage and also must maintain an inventory of each piece of equipment showing current location. Please give as much advance notice as you can.

Clinic Information Security File

As a Clinic ISSM you should maintain a computer security file which includes:

- (1) Applicable security directives
- (2) Clinic ISSM appointment letter
- (3) Current Computer Access Lists
- (4) Attendance record of any security briefs you provide
- (5) Clinic Information Systems Security Guide (this book)
- (6) User Information Systems Security Guide

- (7) Signed off sheet for User Information Systems Security Guide
- (8) Copy of current computer inventory

Sample Forms

Computer Authorized User List

Security Incident Report

Information Systems Security Rules

MEMORANDUM

From: Clinic Information System Security Manager

To: Information System Security Manager, Management Information Department

Subj: COMPUTER AUTHORIZATION ACCESS LIST FOR _____ (AREA)

Ref: (a) SECNAVINST 5239.3

(b) NDCSDIEGOINST 5239.1D

1. In accordance with references (a) and (b), the following list of personnel are authorized to use the computers for _____ (system Bar code(s)/room #) at _____ Branch Clinic.

Name

Rate

2. Only personnel authorized by this access list shall be allowed to utilize the computer equipment in the assigned area. Responsible user may verbally authorize (give permission) to another user temporarily. Any unauthorized person attempting to utilize the clinic computer equipment shall be challenged and reported to the command Information System Security Manager.

3. Post a copy of this access list in a highly visible area that can be seen upon entering the spaces where computers are maintained. In addition, a copy shall also be attached to the side of the computer/monitor terminal.

Clinic Information System Security Manager
Signature Block

Copy to:
ISSM

INFORMATION SYSTEMS SECURITY RULES

Passwords:

DO protect your passwords. DO NOT reveal them to anyone. Notify your clinic Information Systems Security Officer if you suspect or know that your password has been compromised. DO take special precautions when logging on to ensure that your password is not disclosed to other personnel. DO NOT use another person's password or allow anyone to use your password.

Access to Data and Systems:

DO NOT enter, copy, or otherwise process any CLASSIFIED data.
DO access only data required to accomplish your official duties.
DO log off anytime you are going away from your terminal or computer.
DO immediately retrieve and protect all sensitive printed reports or documents from the printer..
DO label all diskettes containing privacy act or sensitive data and store them in a secure location.
DO save your data often while working and make backups any time you make significant additions or changes to your data.

Software:

DO use only NDCSW authorized software.
DO observe all software license agreements.
DO NOT make unauthorized copies of software.
DO NOT use any public domain or shareware software unless it has been authorized and tested by the Management Information Department.

Security Incident Reporting:

DO report immediately all incidents of compromise, suspected compromise, unauthorized access (accidental or deliberate), disclosure of sensitive information or passwords, and related security violations to your clinic Information Systems Security Manager.

User Acknowledgment:

I have read this document and understand my general responsibility in the use and protection of the U. S. Naval Dental Center Southwest and Branch Dental Clinic computer systems, data, and programs. I understand that failure to comply with established Automated Information Systems Security rules may result in administrative and/or disciplinary action.

User Signature

Date

Print User Name

Department/Clinic

Copy to:
Original to clinic ISSM

INFORMATION SYSTEMS SECURITY INCIDENT REPORT

From: _____
Name of individual reporting incident Clinic Telephone #
To: Command Information Systems Security Manger
Via _____
Clinic ISSM Clinic Telephone #

Subj: INFORMATION SYSTEMS SECURITY INCIDENT REPORT

1. Type of security incident:

- Suspected virus infection
- Violation of password
- Violation of terminal security controls
- Violation of microcomputer security controls
- Unauthorized access to restricted area
- Environmental controls failure
- Loss or misuse of hardware
- Loss or misuse of software
- Destruction, disclosure, or alteration of data

Data was: (Check all that apply)

- Privacy Act Sensitive Unclassified Unclassified
- Destruction Disclosure Alteration

2. Location of incident _____ on _____
Dept./Bldg./Room Date Time

3. There __ was __ was not any loss of service.

4. Personnel involved, including witnesses (if applicable):

Name	Rank	Dept.	Telephone
------	------	-------	-----------

5. Use reverse side to document a brief description of security incident.

Signature Date