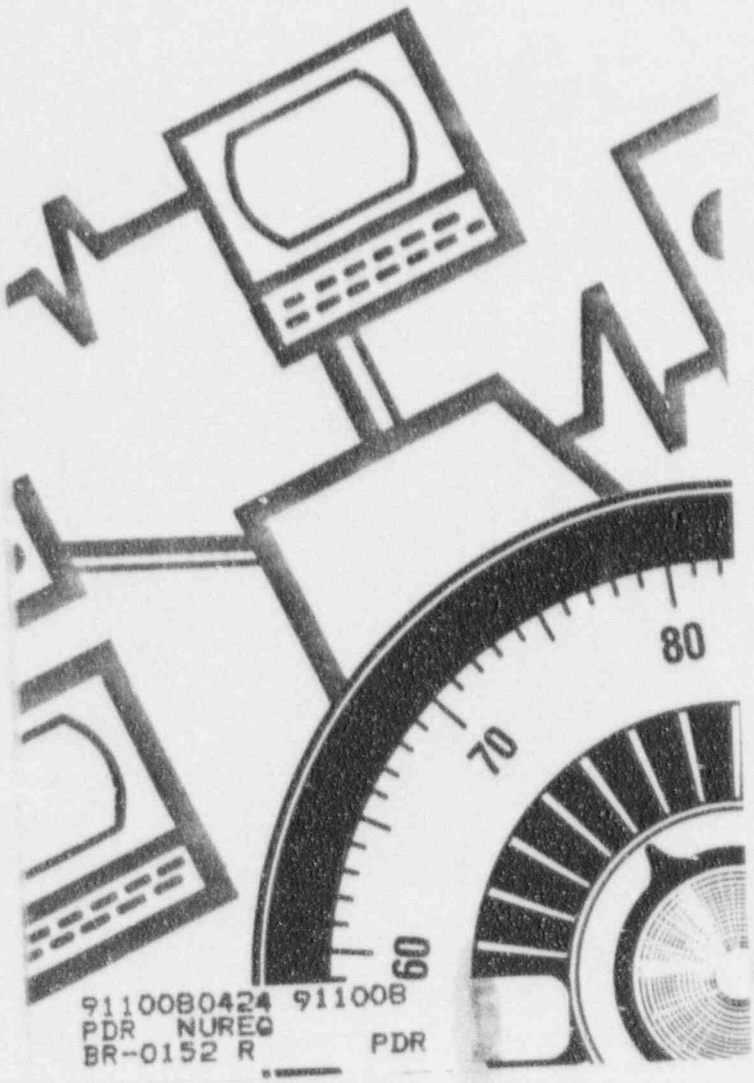
NUREG/BR-0152

LOCAL AREA NETWORK SECURITY GUIDE

GENERAL SECURITY REQUIREMENTS FOR USING LOCAL AREA NETWORKS

U.S. Nuclear Regulatory Commission
Office of Information
Resources Management
Division of Information
Support Services



Local Area Network Security Guide

GENERAL SECURITY REQUIREMENTS FOR USING LOCAL AREA NETWORKS

A Local Area Network (LAN) is a system for linking programs, storage, and devices to multiple work-stations over relatively small geographic areas. Typically, a LAN interconnects computers within a building or a number of buildings in the same area. When a PC or terminal is connected to a LAN, the working environment changes. What was private computing, becomes group computing. In this environment, the LAN is an attractive target for data theft, disclosure, modification, and destruction. Data, programs, and peripherals are shared by everyone on the LAN. New communication routes to corporate data make each PC and work station potentiallly a threat to the integrity, confidentiality, and availability of NRC sensitive and mission critical data.

The following instructions provide a step-by-step approach to entering data and properly securing it in a LAN environment. These instructions are not inclusive; therefore, if you have any questions, contact the Office of Information Resources Management (IRM), Division of Information Support Services (DISS), or refer to NRC Appendix 2301, Parts I and II.

Classified Information

There are no current classified NRC LAN systems and no plans to develop such systems. NEVER, under any circumstances, process or enter classified information or data on a LAN system.

Sensitive Unclassified Information

If sensitive unclassified information is to be entered on a LAN, then take the following steps.

1) Protect Your Equipment

Keep food, drink, and electrical appliances away from LAN equipment, PC, terminal and media.

2) Protect Your Area

Recognize, politely challenge, and assist people who do not belong in the area.

3) Protect Passwords

Use only permitted passwords, change them frequently, and DO NOT share your password with anyone.

4) Protect Your Files

Establish and periodically review access privileges for each LAN-sensitive file. Use system security features to prevent unauthorized access to your LAN files.

5) Protect Your Unattended Terminal

Always logout before leaving your terminal or PC.

6) Protect Against Viruses

Never bring in or use unapproved, unauthorized or personal software at the office.

7) Protect Your Media

Label all diskettes; lock up software, removable media and equipment that contains fixed media.

8) Protect Against Disaster

Disasters start when data and programs are not backed up routinely. Always back-up programs, data and other files and secure them properly.

Unauthorized reproduction of copyrighted software is against the LAW