CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES ADMINISTRATIVE PROCEDURE	Proc. AP–014 Revision 4 Change 0 Page 1 of 7

Computer Network Access and Usage

EFFECTIVITY AND APPROVAL

Revision 4, Change 0 of this procedure became effective 08/02/2004. This procedure consists of the pages and changes listed below.

Page No.	Change	Date Effective
All	0	08/02/2004

Supersedes Procedure No.: AP–014, Rev 3, Chg 2

Approvals

Written By	Date	Concurrence Review	Date
/s/ Perry Seely	08/02/2004	/s/ Arnold Galloway	08/02/2004
Quality Assurance	Date	Cognizant Director	Date
/s/ Robert Brient	08/02/2004	/s/ Pat Mackin	08/02/2004

AP–014 Computer Network Access and Usage

1. INTRODUCTION AND PURPOSE

The Center for Nuclear Waste Regulatory Analyses (CNWRA) operates a computer network to support work performed on behalf of the U.S. Nuclear Regulatory Commission (NRC), and other clients, under various contracts. The network is composed of Sun Microsystems, x86 Personal Computers, and Silicon Graphics computers/workstations on two physical Ethernet segments. Connections are maintained to the NRC and Southwest Research Institute® (SwRI®), which provide access to off-site networks such as the Internet.

Although the terminology used herein reflects that of the UNIX operating system, this procedure applies to all computer systems connected to the network, regardless of their operating system or manufacturer.

2. DEFINITIONS

ARPANet—A research network funded by the Advanced Research Projects Agency (ARPA) to build and test networking protocols for military networks. The results of the research include such protocols as the transmission control protocol/internet protocol (TCP/IP) suite, packet-switch network theory, and battlefield network technology.

Electronic Mail (email)—A method of electronically transferring messages (often including attachments, such as documents, slides, and pictures).

Information Management System (IMS) Group staff member—An employee, consultant, or contractor charged with installation and maintenance of CNWRA computer systems.

Intellectual Property—Information produced or licensed by a particular individual or institution. The right to control the use and release intellectual property is retained by the owner.

Internet—A collection of internetworked networks. This term refers to the global network that is the outgrowth of combining ARPANet and NFSNet [high-speed backbone networks spanning the United States (U.S.) continent] and regional networks (THENet, etc.).

Local Area Network (LAN)—A data communication network connecting electronic office equipment.

Telnet—A method (and program) used to connect to a remote computer system, as if using a terminal directly attached to that system. Used on both the CNWRA LAN and connected networks.

3.0 RESPONSIBILITY

3.1 The Director of Administration is responsible for promulgating, revising, and evaluating compliance with this procedure.

3.2 The IMS Group staff are responsible to operate legally and ethically to keep computing resources operating and available. There is a trade-off between user privacy and the need to ensure the continued functioning of the CNWRA LAN and monitor for violations of law and policy. The IMS group staff will maintain the privacy of user files within these bounds.

3.3 CNWRA users are responsible for any and all activity initiated on CNWRA LAN facilities by anyone using their accounts. Users should not allow others to use their accounts.

4.0 IMS ACTIVITIES

CNWRA computer-related systems are subject to monitoring. IMS Group staff have administrative access to all systems and will examine files, e-mail, and printouts to diagnose and correct problems with system software or hardware.

4.1 The IMS Group staff will monitor computer system use, including individual login sessions, and perform keystroke monitoring, to identify if a user is acting in violation of the policies, regulations, or laws.

4.2 The IMS Group staff will verify the security of user passwords. Users will be notified if their passwords have been compromised, and they will be responsible for defining more secure passwords.

4.3 Backups of data stored on CNWRA computer systems are made on a regular basis to protect against hardware and software failures.

4.4 The IMS Group staff may alter the priority or terminate the execution of any process that is consuming excessive system resources or objectionably degrading system response. The IMS Group staff may terminate login sessions that have been idle (unused) for long periods to free resources. The IMS Group staff will notify the staff member, or the staff member's supervisor, and the CNWRA Director of Administration before taking any such action.

4.5 The IMS Group staff will remove or compress disk files that are consuming large amounts of disk space if there is a critical shortage of storage on a system. When possible, the IMS Group staff will notify the users and work with the to identify alternative storage prior to taking action.

4.6 The IMS Group staff shall provide advance notice of system shut-downs, maintenance, upgrades, or changes so users may plan around periods of system unavailability. In an emergency, the IMS Group staff may shut down a system without advance notification. Users will be provided the opportunity to save work before the system is taken out of service, when possible.

4.7 In the event of a system compromise, any affected systems will be isolated from the network and reloaded, if possible, before being reconnected to the network.

4.8 Upon identifying a violation of this procedure that constitutes an immediate, clear danger to the CNWRA computer systems or data; the System Security Officer (or designee) will limit or suspend the user's access to CNWRA computer resources. The user, immediate supervisor, and CNWRA Director of Administration will be notified of such action as soon as is practical.

5.0 USER ACTIVITIES

5.1 Users shall secure their computers when unattended. This can be accomplished by logging out or locking workstations. For general-purpose or walkup computers, users are responsible for securing machines when unattended and logging off when finished.

5.2 Users are responsible for selecting secure passwords and for keeping them secure from non-authorized users. Passwords should not be written down, stored on-line, or given to others. Passwords should have the following attributes.

- Use a set of alpha-numeric and special characters.
- Have a minimum of 8 characters; one must be a special character, and two must be numbers.
- Change passwords at least every 90 days and no more frequently than 7 days.
- Avoid using any of the last 5 expired passwords.

5.3 Users must report any system security violation, or suspected system security violation, to IMS Group staff members as soon as it is identified.

5.4 Users who borrow hardware, software, or documentation (e.g., laptop computers) are responsible for the proper care of that equipment, and for returning it in a timely manner.

5.5 CNWRA computer-related systems may not be used for the reception, display, processing, storage, or transmission of pornographic, illicit, erotic, or other material of a sexually explicit nature at any time by any user.

5.6 Software shall be used in accordance with the provisions of its license. Users will relinquish shared licensed software when no longer needed.

5.7 Users shall not install or remove software or hardware from their computers.

5.8 Many computer resources, such as disk space, central processing unit cycles, printer queues, batch queues, login sessions, and software licenses, are shared. No user may monopolize these resources. Users should consume as little disk space as practical, compressing files and archiving unused files offline. Batch queues and job priorities shall be used to facilitate computer use by all staff members.

5.9 Users may not intentionally develop or use programs that (i) harass other users of the system; (ii) attempt to bypass system security mechanisms, steal passwords or data, or "crack" passwords; (iii) attempt to consume all of an available system resource (memory, swap space, disk space, network bandwidth, etc.); (iv) attempt to replicate or attach themselves to other programs, commonly called worms or viruses; or (v) evade software licensing or copying restrictions.

5.10 Files of other users are considered private. The ability to read a file does not give permission to read the file. User's may not alter another's files without permission. The ability to alter a file does not give permission to alter a file.

5.11 CNWRA computer systems shall not be used to defame, abuse, threaten, denigrate, insult, or attack any person, company, organization, or institution.

6.0 ACCESS TO CNWRA FACILITIES

6.1 Only persons properly authorized by a CNWRA IMS Group staff member may access CNWRA LAN facilities. Proper authorization requires a user ID and password.

6.2 The LAN facilities of CNWRA are made available to staff members at the time of their employment and are provided for use in support of project work. LAN facilities are also made available, as appropriate, to consultants, subcontractors, temporary employees, and guests to perform project work at the request of the CNWRA manager responsible for that work. Staff members, consultants, subcontractors, and temporary employees will use the CNWRA LAN facilities ethically, legally, and not to the detriment of others. Access to CNWRA computers is a privilege, granted at the CNWRA management discretion.

6.3 Misuse of computing, networking, or information resources may result in the loss of

computing privileges. Additionally, misuse may be a prosecutable offense under applicable laws and regulations. IMS Group staff members will report violations of law to the CNWRA Director of Administration.

6.4 CNWRA LAN facilities may not be used for personal activity that is unrelated to CNWRA business. CNWRA computer related systems may not be used for private gain, political purposes, non-sanctioned charity solicitations, or non-CNWRA business purposes.

6.5 CNWRA LAN facilities and network connections may not be used to make unauthorized connections to, break into, or adversely affect the performance of other computer systems. The ability to connect to other systems via the network does not imply the right to use or connect to these systems unless properly authorized by the owners.

7.0 THE INTERNET AND ELECTRONIC MAIL

7.1 Email is not secure or guaranteed. Users should not include or append private, confidential, or predecisional information in e-mail delivered via the Internet. Users may include or append predecisional data or information to e-mail sent to the NRC staff via the secure Frame-Relay connection with NRC. E-mail should be routinely deleted or saved as hard copy in accordance with the CNWRA records retention policy in AP–019. Users should exercise caution when opening e-mail attachments from unknown individuals, as they may contain malicious programs.

7.2 Users will practice accepted business etiquette while participating on the Internet.

8.0 INTELLECTUAL PROPERTY, SOFTWARE COPYRIGHT, AND LICENSES

8.1 Unless covered by other copyright or ownership, all CNWRA computers, networks, programs, and data residing on or processed by them, are the property of the CNWRA. CNWRA ownership includes all files, documents, e-mail, mass storage disks, diskettes, tapes, and other storage media.

8.2 CNWRA intellectual property includes all documents, messages, notes, programs, etc., created using CNWRA computer systems or facilities, or while performing CNWRA work. CNWRA intellectual property also includes NRC, SwRI, and CNWRA sensitive, business-confidential, predecisional, and proprietary materials. All users shall protect CNWRA intellectual property consistent with its level of sensitivity. CNWRA intellectual property shall be used only in the manner prescribed in its accompanying documentation. CNWRA intellectual property shall not be released to unauthorized recipients.

8.3 Non-CNWRA intellectual property includes intellectual property owned by other organizations or persons and obtained or licensed for use by CNWRA computer systems or personnel in performance of CNWRA work. Non-CNWRA intellectual property shall only be used in the manner prescribed in its accompanying documentation. Non-CNWRA intellectual property shall not be released to unauthorized recipients.

8.4 It is against federal law and CNWRA policy to violate the copyrights or patents on computer software. It is against CNWRA policy and may be a violation of the law to violate software license agreements.

8.5 Licensed software may not be used on personal (home) computers, unless the specific license permits.

8.6 Source code for licensed software may not be included in software that is released for use outside CNWRA, unless explicitly authorized by the licensor.

8.7 The use of “freeware” and “shareware” software packages on the CNWRA LAN is prohibited unless specifically authorized and installed by the CNWRA IMS Group staff.

8.8 Use of commercial off the shelf software that has been “cracked” to circumvent the licensing requirements of the software manufacture is not permitted. Software provided by the government or sponsored by the government may only be used in accordance with its specified terms.