7-1-2001

UAP 2510: Computer Use Guidelines (Now 2520)

University of New Mexico

The University of New Mexico

University Business Policies and Procedures Manual

MOVED to Policy 2520

2510
COMPUTER USE GUIDELINES
Effective Date: July 1, 2001

This version
was Distributed
for the period
of: 7-1-01 to: 7-1-61

1. General

The University of New Mexico provides computing services to faculty, staff, students, retirees, and specified outside clients of the University. "Acceptable Computer Use" Policy 2500, UBP describes the University's policies pertaining to allowable use, misuse, user rights and responsibilities, and privacy limitations. This document supplements policy 2500 by providing guidelines for confidentiality and privacy, copyrights, computer accounts and passwords, computer and data security, electronic communications, and networks.

2. Confidentiality and Privacy

Everyone, including managers, supervisors, and systems administrators, shall respect and protect the privacy of others. "Acceptable Computer Use" Policy 2500, UBP defines the limited conditions under which access to information and files can be obtained. Although the University is committed to protect individual and information privacy, correspondence and information stored and transmitted through University computer networks and systems cannot be guaranteed to be private. Since confidential information is often stored on desktop machines, displayed on screens, or printed on paper that could be in public view, users need to control access by:

- using passwords;
- turning screens away from public view;
- logging out of systems when leaving the work area;
- shredding reports containing private information prior to disposal; and
- clearing confidential information off desks in public areas.

3. Copyrights

Laws that protect owners of intellectual, textual, music, sound, photographic, artistic, and graphic property apply to all computer media such as software, electronic library material, and paid subscriptions. The University is committed to protect copyrights.

3.1. Software Copyrights

Commercial programs produced for use on computers are protected by copyright. Copying computer software without authorization violates federal copyright law. Payment for a software product represents a license fee to use a designated number of copies. The buyer does not own the software, but merely buys a license to use the software. The license is not a blanket authorization to copy.

3.1.1. Site Licenses

The University enters into site license agreements with commercial vendors for campus-wide use of certain software products. The University currently has site licenses for products, including word-processing, spreadsheet, and database management applications software. Before buying a particular product, departments should contact the University Purchasing Department or CIRT Software Distribution to determine if the University has a site license or volume purchase discounts for the software in question. In addition, many software applications are available at an educational discount through the UNM Bookstore or other vendors.

3.2. Software Developed Internally

University personnel may develop computer programs using University resources. Such software may be subject to the University's Intellectual Property Policy.

4. Computer Accounts and Passwords

The University through CIRT and departments provides computer accounts to authorized users for access to various University systems. These accounts are a means of operator identification and passwords are used as a security measure. Account use is a privilege not a right.

4.1. Account Authentication

Passwords, PINs, and other identifiers authenticate the user's identity and match the user to the privileges granted on University computer networks and systems. A password is a security measure designed to prevent unauthorized persons from logging on with another person's computer account and reading or changing data accessible to that user. Users should create passwords carefully and handle them with care and attention. Refer to www.unm.edu/cirt/accts/ for guidance on creating passwords. For this security feature to be effective the user must protect the secrecy of his/her password. Each user should:

- change his/her password regularly and at any time the user feels the password may have been compromised;
- avoid writing the password down;
- not disclose or share the password with anyone; and.
- choose a password that is easy to remember but hard to guess.

Similar measures apply to all authentication methods such as PINs.

4.2. Account Termination and Locking

When an individual leaves the University, his or her account(s) will be locked and eventually deleted. If misuse or theft is detected or suspected, account(s) will be locked according to the University's procedures.

5. Computer and Data Security

Everyone at the University shares responsibility for the security of computer equipment and information.

5.1. Physical Security

Everyone is responsible for the proper use and protection of University computer equipment. Examples of protection measures include:

- locking areas after business hours or at other times when not in use;
- taking special precautions for high-value, portable equipment; and
- following University policies for taking computer equipment off campus (refer to "Taking University Property Off Campus" Policy 7730, UBP).

5.2. Information Security

Security of information is an essential responsibility of computer system managers and users alike. For example users are responsible for:

- ensuring the routine backup of their files;
- using data only for approved University purposes; and
- ensuring the security and validity of information transferred from University systems.

5.3. Computer Viruses

Due to the proliferation of computer viruses and the damage they can cause, the University strongly recommends that users keep current anti-viral software active and scan frequently for viruses. For example scan the following for viruses:

- attachments
- downloaded files; and
- shared diskettes, CDs, and other media.

For additional information on anti-viral software, contact **www.unm.edu/cirt/virus.html**.

6. Electronic Communications

Electronic communications include information in any form such as data, audio, video, and text that is conveyed or stored electronically, for example, by e-mail, web pages, and in files. Electronic communications are used for furthering the education, research, and public service mission of the University and may be used for **incidental personal use**, but may not be used for commercial purposes or profit-making. The following types of communication are prohibited:

- chain letters, pyramid schemes, and unauthorized mass mailings;
- fraudulent, threatening, defamatory, obscene, harassing, or illegal materials;

- non-work or non-class related information sent to an individual who requests the information not be sent;
- copyright law violation; and
- commercial or personal advertisements, solicitations, promotions, destructive programs, or any other unauthorized use.

Users should understand that, due to their nature, electronic communications can be intentionally or unintentionally viewed by others or forwarded to others, and are therefore inherently not private. In addition, addressing errors, system malfunctions, and system management may result in communications being viewed and/or read by other individuals and/or system administrators. CIRT provides assistance in the proper use of e-mail at www.unm.edu/cirt/email/.

6.1. Identification

Anonymous speech is allowed; however, misrepresenting or forging a user's identity in order to deceive is prohibited. Users must state whether they are speaking for themselves or in an official capacity for the University. Electronic communications that represent the University sent to non UNM addresses must be done in a professional manner and comply with **"University External Graphic Identification Standards" Policy 1010, UBP.**

7. Use of the University Network

The University network is large and complex and supports mission critical functions such as patient care, payroll, academic classes, Internet access, and electronic mail. To ensure the integrity of the network and maximize the availability of network services, all users connected to the University's network (CDCN) by dialing in, direct connection, or departmental sub network must follow CIRT's requirements which can be found at www.unm.edu/cirt/connections.

Comments may be sent to UBPPM@UNM.edu
http://www.unm.edu/~ubppm