Executive Memorandum No. 16

Policy for Responsible Use of University Computers and Information Systems

1. Purpose

   It is the purpose of this Executive Memorandum to set forth the University's administrative policy and provide guidance relating to responsible use of the University's electronic information systems.

2. General

   The University of Nebraska strives to maintain access for its faculty, staff, students, administrators and Regents (the "users") to local, national and international sources of information and to provide an atmosphere that encourages sharing of knowledge, the creative process and collaborative efforts within the University's educational, research and public service missions. Access to electronic information systems at the University of Nebraska is a privilege, not a right, and must be treated as such by all users of these systems. All users must act honestly and responsibly. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements related to University information systems. All users shall act in accordance with these responsibilities, and the relevant local, state and federal laws and regulations. Failure to so conduct oneself in compliance with this Policy may result in denial of access to University information systems or other disciplinary action.

   The University of Nebraska is a provider of a means to access the vast and growing amount of information available through electronic information resources. The University of Nebraska is not a regulator of the content of that information and takes no responsibility for the content of information, except for that information the University itself and those acting on its behalf create. Any persons accessing information through the University of Nebraska information systems must determine for themselves and their charges whether any source is appropriate for viewing.

   Accepting any account and/or using the University of Nebraska's information systems shall constitute an agreement on behalf of the user or other individual accessing such information systems to abide and be bound by the provisions of this Policy. The University may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of University policies or state or federal laws. When it has been determined that there has been a violation, the University may restrict or prohibit access by an offending party to its information systems through University-owned or other computers, remove or limit access to material posted on University-owned computers or networks, and, if warranted, institute other disciplinary action.

3. Definitions

   For purposes of this policy the following definitions shall apply:

   a. Electronic communications shall mean and include the use of information systems in the communicating or posting of information or material by way of electronic mail, bulletin boards,

World Wide Web (internet), or other such electronic tools.

b. Information systems shall mean and include computers, networks, servers and other similar devices that are administered by the University and for which the University is responsible. "Networks" shall mean and include video, voice and data networks, routers and storage devices.

c. Obscene with respect to obscene material shall mean (1) that an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion, (2) the material depicts or describes in a patently offensive way sexual conduct specifically set out in Neb. Rev. Stat. §§ 28-807 to 28-809, as amended, and (3) the material taken as a whole lacks serious literary, artistic, political, or scientific value.

4. Permitted Uses

a. University Business Use and Limited Personal Use.

University information systems are to be used predominately for University-related business. However, personal use is permitted so long as it conforms with this Policy and does not interfere with University operations or an employee user's performance of duties as a University employee. As with permitted personal use of telephones for local calls, limited personal use of information systems does not ordinarily result in additional costs to the University and may actually result in increased efficiencies. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material is prohibited. UNDER ALL CIRCUMSTANCES, PERSONAL USE BY EMPLOYEES MUST COMPLY WITH SUBSECTION b. OF THIS SECTION AND SHALL NOT CONFLICT WITH AN EMPLOYEE'S PERFORMANCE OF DUTIES AND RESPONSIBILITIES FOR THE UNIVERSITY. Personal use may be denied when such use requires an inordinate amount of information systems resources (e.g. storage capacity).

b. Prior Approval Required for Personal Use for Outside Consulting, Business or Employment.

Personal use of University information systems resources or equipment by any user for personal financial gain in connection with outside (non-University) consulting, business or employment is prohibited, except as authorized for employees by Section 3.4.5 of the Bylaws of the Board of Regents. Employee personal use in conjunction with outside professional consulting, business or employment activities is permitted only when such use has been expressly authorized and approved by the University Administration or the Board of Regents, as appropriate, in accordance with the requirements of said Section 3.4.5 of the Bylaws.

5. Access

Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relation with the University of Nebraska, his or her ID and password shall be denied further access to University computing resources.

6. Misuse of Computers and Network Systems

Misuse of University information systems is prohibited. Misuse includes the following:

a. Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.

b. Accessing without proper authorization computers, software, information or networks to which the University belongs, regardless of whether the resource accessed is owned by the University or the abuse takes place from a non-University site.

c. Taking actions, without authorization, which interfere with the access of others to information systems.

d. Circumventing logon or other security measures.

e. Using information systems for any illegal or unauthorized purpose.

f. Personal use of information systems or electronic communications for non-University consulting, business or employment, except as expressly authorized pursuant to Section 3.4.5 of the Bylaws of the Board of Regents.

g. Sending any fraudulent electronic communication.

h. Violating any software license or copyright, including copying or redistributing copyrighted software, without the written authorization of the software owner.

i. Using electronic communications to violate the property rights of authors and copyright owners. (Be especially aware of potential copyright infringement through the use of e-mail. See the provisions under "E-Mail" contained in this Policy.)

j. Using electronic communications to harass or threaten users in such a way as to create an atmosphere which unreasonably interferes with the education or the employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to University users.

k. Using electronic communications to disclose proprietary information without the explicit permission of the owner.

l. Reading other users' information or files without permission.

m. Academic dishonesty.

n. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards, or other documents or property).

o. Using electronic communications to hoard, damage, or otherwise interfere with academic resources available electronically.

p. Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work.

q. Using electronic communications to fabricate research data.

r. Launching a computer worm, computer virus or other rogue program.

s. Downloading or posting illegal, proprietary or damaging material to a University computer.

t. Transporting illegal, proprietary or damaging material across a University network.

u. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material.

v. Violating any state or federal law or regulation in connection with use of any information system.

7. Privacy

a. User Privacy Not Guaranteed. When University information systems are functioning properly, a user can expect the files and data he or she generates to be private information, unless the creator of the file or data takes action to reveal it to others. Users should be aware, however, that no information system is completely secure. Persons both within and outside of the University may find ways to access files. ACCORDINGLY, THE UNIVERSITY CANNOT AND DOES NOT GUARANTEE USER PRIVACY and users should be continuously aware of this fact.

b. Repair and Maintenance of Equipment. Users should be aware that on occasion duly authorized University information systems technological personnel have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment the University deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for University needs. Information systems technological personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

c. Response to a Public Records Request, Administrative or Judicial Order or Request for Discovery in the Course of Litigation. Users should be aware that the Nebraska public records statutes are very broad in their application. Certain records, such as unpublished research in progress, proprietary information, personal information in personnel and student records are protected from disclosure. However, most other University records contained in electronic form require disclosure if a public record request is made. Users should remember this when creating any electronic information, especially e-mail. Also, users should be aware that the University will comply with any lawful administrative or judicial order requiring the production of electronic files or data stored in the University's information systems, and will provide information in electronic files or data stored in the University's information systems in response to legitimate requests for discovery of evidence in litigation in which the University is involved.

d. Response to Misuse of Computers and Network Systems. When for reasonable cause, as such cause may be determined by the Office of the Vice President and General Counsel, it is believed that an act of misuse as defined in section 6 above has occurred, then the chief information services officer serving Central Administration or serving the relevant campus may access any account, file or other data controlled by the alleged violator and share such account information, file or other data with those persons authorized to investigate and implement sanctions in association with the misuse of the University's computer and information systems. Should any of the chief information service officers reasonably believe that a misuse is present or imminent such that the potential for damage to the system or the information stored within it, is genuine and serious (e.g. hacking, spamming or theft), then the chief information officer may take such action as is necessary to protect the information system and the information stored in it, including the denial of access to any University or non-University user, without a determination from the Office of the Vice President and General Counsel regarding reasonable cause; provided however, that the chief information officer shall contact the Office of the Vice President and General Counsel as soon as possible to confirm that any protective actions taken were appropriate and within the parameters of this executive memorandum.

e. Access to Information Concerning Business Operations. Employees regularly carry out the business functions of the University using the University's information systems. business records, inquiries and correspondence are often stored such that individuals may control the access to particular information stored within the University's information system. Should any employee become unavailable, be incapacitated due to illness or other reasons, or refuse to provide the information necessary to carry out the employee's job responsibilities in a reasonably timely manner, then following consultation with and approval by the Office of the Vice President and General Counsel, the chief information officer of Central Administration or of the relevant campus may access the employee's records in order to carry out University business operations on behalf of the unavailable or uncooperative employee.

8. E-mail

a. Applicability. ALL POLICIES STATED HEREIN ARE APPLICABLE TO E-MAIL. E-mail should reflect careful, professional and courteous drafting-particularly since it is easily forwarded to others. Never assume that only the addressee will read your e-mail. Be careful about attachments and broad publication messages. Copyright laws and license agreements also apply to e-mail.

b. E-mail Retention. E-mail messages should be deleted once the information contained in them is no longer useful. When e-mail communications are sent, the e-mail information is stored in one or more backup files for the purposes of "disaster recovery", i.e. inadvertent or mistaken deletions, system failures. In order to provide for the recovery of deleted e-mail, while maintaining efficient use of storage capabilities, e-mail information on backup files shall be retained for a period of time not to exceed seven days.

9. Web Pages

The Central Administration and each University campus may establish standards for those Web Pages considered to be "official" pages of the University. All official Web Pages shall contain the administrative unit's logo in the header and footer in order to identify it as an official University of Nebraska Web Page. No other Web Pages shall be allowed to use University of Nebraska logos without the express permission of the University.
Originators of all Web Pages using information systems associated with the University shall comply with University policies and are responsible for complying with all federal, state and local laws and regulations, including copyright laws, obscenity laws, laws relating to libel, slander and defamation, and laws relating to piracy of software.

The persons creating a Web Page are responsible for the accuracy of the information contained in the Web Page. Content should be reviewed on a timely basis to assure continued accuracy. Web Pages should include a phone number or e-mail address of the person to whom questions/comments may be addressed, as well as the most recent revision date.

10. Notification

This Policy shall be published in all employee and faculty handbooks and student catalogs, and placed on the World Wide Web in order to fully notify users of its existence.

11. Application and Enforcement

This Policy applies to all administrative units of the University of Nebraska. The Central Administration and each University campus is encouraged to provide supplemental policy guidance, consistent with this Policy, designed to implement the provisions herein.

Each University campus shall be responsible for enforcing this Policy in a manner best suited to its own organization. It is expected that enforcement will require cooperation between such departments as computer systems administration, human resources, affirmative action, academic affairs and student affairs. Prior to any denial of access or other disciplinary action, a user shall be provided with such due process as may be recommended by the University's Office of the General Counsel.

Reference: August 28, 2001