April 17, 1991

REPORT OF THE UW-MADISON AD HOC ELECTRONIC DATA ADVISORY COMMITTEE

INTRODUCTION

The Electronic Data Advisory Committee was created by the University Committee to clarify the privacy and confidentiality status of electronic data and to draft procedures for the University to follow in providing access to this form of information.

The faculty and staff of the University should be under no delusions as to the essential confidentiality of their electronic files. Even when one takes elaborate precautions (e.g., file encryption) the nature of modern communication networks is such that true confidentiality is impossible to guarantee. All users of these services should be apprised of this fact.

The Federal Electronic Communications Privacy Act of 1986 and parallel language adopted by the Wisconsin Legislature allows the University to examine electronic information when necessary to protect the rights and property of the University. The proposed procedures provide a mechanism for doing so in a way that respects the rights of individuals involved.

The report that follows deals with the question of appropriate procedures for the University to follow. In general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to

1. meet the requirements of the state open records law;
2. protect the integrity of University services and the rights and property of the State;
3. allow system administrators to perform routine maintenance and respond to emergency situations such as combating "viruses" and the like; and
4. protect the rights of individuals working in collaborative situations where information and files are shared.

The procedures are based on three fundamental principles:

1. Intrusion into electronic files requires carefully considered cause;

2. Owners of files must be notified before accessing their files; and

3. The University has an obligation to protect the integrity of University services and the rights and property of the State.

DEFINITIONS

As used in these procedures:

1. "Electronic File" encompasses information stored and/or transmitted in electronic form, including but not limited to text, data, sound, graphics, images, and video, irrespective of its recording and transmission media or its format.

   Examples of electronic files include e-mail messages, databases, and magnetic tape files and subsets thereof.

2. "Owner of a file" is defined as follows:

   a. on a single user computer under the control of a single person (e.g., a computer in a faculty office) the files normally belong to that person;

   b. on computers accessed by more than one individual, but which do not have an operating system that identifies files with a specific user, the individual responsible to the University for control of the computer (e.g., the laboratory director or department chair) is considered to be the owner of electronic files resident on that computer;

   c. On multiuser systems, an individual is typically registered or given an account. The registered user or account holder is normally considered to be the owner of files held in that account;

d. In "work for hire" situations where one party enters or edits material for the originator of a file, the one responsible for originating the material in the file is the owner of the file. The person charged with entering the material is usually considered to be an authorized user. For example, when a secretary or a research assistant working under explicit directions uses a computer to enter and edit a document for a faculty member, the faculty member is the owner of the file and the secretary or research assistant is an authorized user.

3. "Authorized User" includes the owner of a file or someone who is given explicit access to the file by an owner.

4. "System Administrator" is an individual who has been charged by a University unit with maintaining a computer system and its software at an acceptable level of performance for the service that it is expected to provide.

PROCEDURES FOR ACCESS TO ELECTRONIC FILES

1. Except as provided for in Section 5, no one but an authorized user of an electronic file may intentionally access the contents of that file without receiving either

   a. The permission of the owner of the file; or

   b. The express written permission of the Vice Chancellor for Academic Affairs, who may grant such permission only in accordance with the procedures established by Sections 2, 3, and 4 below.

2. Except as provided for in Section 6, the Vice Chancellor for Academic Affairs may grant permission to those persons listed in section 2(b) to access a computer or electronic file only upon determining that the following steps have been taken:

   a. The Vice Chancellor for Academic Affairs has received in writing a request for access that specifies the reasons for the requested access and lists the requested file(s) by name, contents, or a description that clearly limits access to the file(s) necessary to further the purposes designated in Section 2(f).

b. The written request has been made by either

   i. the University's Custodian of Records or

   ii. a dean, director, department chair, vice-chancellor, or other person specifically charged with protecting the integrity of University services and the rights and property of the State.

c. The Vice Chancellor for Academic Affairs has notified in writing the owner of the file(s) that a request for access to the specified file(s) has been made and is pending. When there is doubt as to the ownership of a file, notice should be sent to all individuals likely to have an ownership interest.

   Notification must, at a minimum,

   i. specify the name of the party requesting the file(s);

   ii. list by name, description, or contents the file(s) requested;

   iii. indicate that unless waived in writing by the owner of the file(s) within four days of notification, an inquiry as specified in section 2(d) of these procedures will be held to examine whether justification exists for granting the requested access;

   iv. indicate that the owner of the file(s) has a right to make known to the section 2(d) ad hoc committee his or her views on whether access is justified;

   v. indicate that the file(s) in question shall not be altered or deleted; and

   vi. if relevant, indicate that the Vice Chancellor for Academic Affairs has exercised his or her power under section 3 to take the minimum steps necessary to preserve the contents of the subject file(s).

d. The Vice Chancellor for Academic Affairs has appointed an ad hoc committee of three members, all of whom are otherwise uninvolved in the request and at least two of whom are members of the faculty or academic staff (as is appropriate to the case), to inquire into whether a justification under section 2(f) exists to warrant granting the requested access. Unless granted additional time, the ad hoc committee will conduct its inquiry and make a written report to the Vice Chancellor within ten days of its appointment.

At a minimum, the committee shall

i. examine the written request for access provided to the Vice Chancellor under Section 2(a);

ii. if it determines it needs to do so, inquire further of the Section 2(b) person requesting access to the file; and

iii. offer all those notified under Section 2(c) an opportunity to make known to the ad hoc committee their views on whether access is justified.

e. The Vice Chancellor for Academic Affairs has received the results of the inquiry specified in Section 2(d) of these procedures or has received the owner's waiver of the section 2(d) inquiry.

f. The Vice Chancellor for Academic Affairs finds that the requested access is necessary

i. to assure University compliance with the state open records law; or

ii. to protect the integrity of University services and the rights and property of the State.

g. The Vice Chancellor for Academic Affairs has put in writing, with as much specificity as possible, the reasons for granting access to the file(s).

3. Upon the written request of one of those persons listed in section 2(b) or on his or her own initiative, the Vice Chancellor for Academic Affairs may authorize the appropriate University unit to take all necessary steps to preserve and save the contents of any file(s) within the University's computer systems. An order to preserve the contents of the file is meant to assure that the data in the file(s) is not destroyed, altered, or lost. Any such order does not constitute permission to access the contents of the file(s). Access to the contents of the file(s) is expressly prohibited except under the procedures specified by these procedures or the conditions stated in Section 5.

4. All requests for access to electronic files made under the Wisconsin open records law shall be made through the office of the University's Custodian of Records. It is recommended that the office of the Custodian of Records promulgate rules not in conflict with the principles expressed in these procedures.

5. Nothing in these procedures is meant

   a. to interfere with the usual procedures followed by departments and schools in monitoring student accounts given for specific course work; or

   b. to preclude computer system administrators from authorizing the routine maintenance of campus computer or communication systems or the rectification of emergency situations that threaten the integrity of campus computer or communication systems, provided that use of accessed files is limited solely to maintaining or safeguarding the system or solving specific problems.

6. Nothing in these procedures is meant to govern access to files specifically dealt with by Wisconsin or United States statute, such as patient records, student information files, or certain personnel actions.

April 17, 1991

The Ad Hoc Electronic Data Advisory Committee:

Seymour Parter, Professor, Computer Sciences and Mathematics, Chair
David Brown, Senior Policy and Planning Analyst, Office of Information Technology
Dennis Fryback, Professor, Industrial Engineering and Preventive Medicine
Thomas Palay, Professor, Law
Tad Pinkerton, Director, Office of Information Technology and Professor, Computer Sciences
Charlene Rieck, Information Processing Consultant, College ofAgriculture and Life Sciences