II-323
POLICIES AND PROCEDURES GOVERNING ACCESS TO ELECTRONIC FILES

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 information in this form.

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. In addition, the Wisconsin open records law may require public disclosure of electronic data. All users of these services should be apprised of these facts.

The Federal Electronic Communications Privacy Act of 1986 (18 U.S.C. sec. 2511) and parallel language adopted by the Wisconsin Legislature (sec. 968.31(2), Wis. Stats.) 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 cases of requests for access to electronic files initiated internally. (Requests for access that originate external to the university will normally arise under circumstances described in Section 6 of these procedures. In such cases, the university will provide notice to the controller and the opportunity to respond, whenever possible.)

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 and other statutory or regulatory requirements;

2. protect the integrity of the university 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.

Accordingly, the Ad Hoc Electronic Data Advisory Committee recommends the following actions:

1. The university should make a special and periodic effort to notify users that:

    a. Faculty Policies and Procedures include rules governing the privacy of electronic data;

    b. State or federal regulations may supersede these policies and procedures; and

    c. electronic communications and data files are not secure from unauthorized access;

2. Because the proposed policy does not address how departments and schools may access students’ instructional accounts, departments and schools should codify their procedures for managing and gaining access to such accounts;

3. The faculty adopt the following policy and procedures to govern access to electronic files controlled by faculty and staff:

PRINCIPLES

The procedures are based on three fundamental principles:

1. Intrusion into electronic files requires carefully considered cause;

2. Controllers of files should be notified before accessing their files; and

3. The university has an obligation to protect the integrity of the university, its services, its confidential data, 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. "Controller 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 are controlled by 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 controller 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 controller 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 controller 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 controller of the file and the secretary or research assistant is an authorized user.

3. "Authorized User" includes the controller of a file and someone who is given explicit access to the file by a controller.

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

1. Except as provided for in Sections 5 and 6, no one but an authorized user of an electronic file may intentionally access that file without receiving either

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

   b. The express written permission of the vice chancellor for academic affairs and provost, who may grant such permission only in accordance with the procedures established by Sections 2 and 3 below.

2. Except as provided for in Sections 5 and 6, the vice chancellor for academic affairs and provost may grant permission to those persons listed in section 2(b) to access a computer or electronic file only upon determining that the all of the following steps have been taken:

   a. The vice chancellor for academic affairs and provost 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 a dean, director, department chair, vice chancellor, or other person who has responsibility for protecting the integrity of the university, its services, and the rights and property of the State.

   c. The vice chancellor for academic affairs and provost has notified in writing the controller 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 who is the controller of a file, notice should be sent to all the known individuals likely to have such an 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 controller 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 in the event a section 2(d) committee has been appointed, the controller of the file(s) has a right to make known to the committee his or her views on whether access is justified;

      v. indicate that the file(s) in question shall not be altered or deleted by anyone, including the controller and that alterations or deletions may be a basis for disciplinary action; and,

      vi. if relevant, indicate that the vice chancellor for academic affairs and provost 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 and provost has appointed a 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 committee will conduct its inquiry and make a written report to the vice chancellor within ten calendar days of its appointment.

At a minimum, the committee shall

i. examine the written request for access provided to the vice chancellor and provost under Section 2(a); and

ii. 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 and provost has received the results of the inquiry specified in Section 2(d) of these procedures or has received the controller's waiver of the section 2(d) inquiry.

f. The vice chancellor for academic affairs and provost finds that the requested access is necessary to protect the integrity of the university, its services, and the rights and property of the State.

g. The vice chancellor for academic affairs and provost 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 and provost 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 open, read, or otherwise use the contents of the file(s). Access to the contents of the file(s) shall be obtained only under procedures specified herein or under conditions stated in Sections 5 and 6.

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 procedures consistent with the Wisconsin open records law and the principles expressed in these procedures. Such procedures shall provide for notice to the controller before public disclosure, whenever possible.

5. Nothing in these procedures is meant

a. to supersede 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 (which may include safeguarding the system from illegal use) or solving specific problems.

6. Nothing in these procedures is meant to either limit or expand access to files pursuant to Wisconsin or United States statutes or regulations, such as those governing patient records, student information files, open records, criminal investigations conducted by federal, state or local law enforcement authorities or certain personnel actions.

[UW Madison Faculty Document 890a 7 October 1991]