Privacy in the Electronic Environment

Summary/Purpose

This policy provides general principles that help to define the expectations of privacy with regard to electronic information at the University of Mississippi (UM).

I. Preliminary Observations

The University of Mississippi (UM) affirms that the mutual trust and freedom of thought and expression essential to the academic mission of a university rest on an expectation of privacy, and that the privacy of those who work, study, teach, and conduct research in a university setting will be respected. UM recognizes that as faculty, staff and students create, use and store more information in electronic form, there is growing concern that information the user or creator considers private may be more vulnerable to invasion than information stored in more traditional media. This policy highlights some general principles that should help to define the expectations of privacy of those in the UM community. While no document addressing the fluid issue of technology can be exhaustive or inflexibly dictate outcomes in all circumstances, this policy attempts to articulate current practices and provide guidance, so that individuals may make informed and appropriate decisions concerning their various interactions in the electronic environment.

Before addressing these issues, it should also be noted that in carrying out their operations, various UM departments accumulate information about members of its community, e.g., for purposes of payroll, employment or enrollment. Data are also created, though not necessarily compiled or retained on a personally identifiable basis, as an incident to the use of technology, e.g., the charging of purchases on Ole Miss Express cards or the borrowing of library books. UM does not condone disclosure or release of such personal information stored or transmitted through UM systems, except for legitimate purposes as outlined in this policy. It is the responsibility of all UM offices that manage electronic information to safeguard this information from improper disclosure. This involves communicating with employees, including student workers, about this and related policies and training them in the proper handling of personal information as is described in the Information Confidentiality/Security Policy. It is never acceptable to store confidential data such as grades, social security numbers, private correspondence, classified research, etc. on externally hosted systems, including cloud-based storage systems, without a contract that is fully vetted for compliance with UM policies.

Those responsible for maintaining UM's computers and electronic networks have an important and special responsibility to recognize when they may be dealing with sensitive or private information. They may access such information without the user's consent and without obtaining higher level approval, but only when necessary to fulfill their official responsibilities, and they are expected to carry out their duties in ways that are not unreasonably intrusive. They will be subject to disciplinary action if they misuse their access to personally identifiable data or to individuals' personal files, email and voice mail or otherwise knowingly act in ways counter to UM policies and applicable laws.

Finally, this policy should be understood in light of the many other UM policies and laws that bear on individuals' rights to privacy and the institution's responsibilities with respect to information in its possession about individuals. Examples of applicable laws include the Family Educational Rights and Privacy Act of 1974 (the "Buckley Amendment"), the Electronic Communications Privacy Act of 1986, and medical records regulations promulgated under the Health Insurance Portability and Accountability Act of 1996. Examples of applicable UM policies include the IT Appropriate Use Policy and the Information Confidentiality/Security Policy.

II. Policy on Information Created, Stored or Transmitted Through University Electronic Media

A. In General

UM provides collaboration tools, computers, computer and email accounts, networks and telephone systems to faculty members, staff and students for the purpose of furthering UM's academic mission and conducting university business. While incidental and occasional personal use of such systems, including email, and voice mail, is permissible, personal communications and files transmitted over or stored on UM systems are not treated differently from business communications; there can be no guarantee that such personal communications will remain private or confidential (*see Appendix 1*).

As is the case for information in non-electronic form stored in UM facilities, UM's need for information will be met in most situations by simply asking the author or custodian for it. UM reserves the right, consistent with this policy, to access, review and release electronic information that is transmitted over or stored in university systems or facilities. When questions arise about such access, review or release of information, UM commits to treat electronic information no differently from non-electronic information. As with paper information, it is often the case by custom or rule that electronic files are shared and properly accessible by multiple parties in office settings. Where that is the case, the special provisions for access and notification outlined here need not be followed. In other cases, properly authorized UM officials including the Chief Information Officer and the IT Security Coordinator may access email, voice mail or other UM accounts without the consent of the assigned user when there is a reasonable basis to believe that such action:

1. Is necessary to comply with legal requirements or process, or
2. May yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected serious infraction of UM policy (for example alleged research misconduct, plagiarism or harassment), or
3. Is needed to maintain the integrity of UM computing systems, or
4. May yield information needed to deal with an emergency, or

5. In the case of staff, will yield information that is needed for the ordinary business of the university to proceed.

Except as may otherwise be dictated by legal requirements, individuals will be notified of access to, or disclosure of, the contents of their email, voice mail or their accounts as soon as practicable. In cases where such notification might jeopardize an ongoing investigation of suspected wrongdoing it may be delayed until the conclusion of the investigation. The investigating entity, whether authorized through internal auditing, the IT Security Coordinator, the Chief Information Officer or others as appointed by the Chancellor, is responsible for maintaining an official record of all electronic data searches for a period of one year. A copy of the records will be provided to the office of the University Attorney upon request. All questions regarding investigations shall be directed through the University Attorney's office.

B. Faculty

UM has the utmost respect for the freedom of thought and expression that are at the core of the academic mission. Whenever possible, therefore, UM will resolve any doubts about the need to access a UM computer or other systems in favor of a faculty member's privacy interest. Computer files, email and voice mail created, stored, transmitted or received by faculty will be afforded the same level of privacy as the contents of their offices. Section 25-65-17 of the Mississippi Code states that "internal audit staff shall have access to all personnel and any records, data and other information of the university, community/junior college or state agency deemed necessary to carry out assigned duties." Except as may otherwise be dictated by legal requirements, the procedures outlined in that policy will be followed with respect to a faculty member's computer files, email or voice mail in connection with other investigations or proceedings.

C. Staff

It is generally not UM policy to access staff members' electronically stored information. As noted above, UM's need for information will normally be met by asking an employee for it. Properly authorized university officials, including supervisors acting with the consent of their management, may, however, access, review and release the contents of staff computer files, email or voice mail transmitted over or stored on UM systems when, for example, an employee is absent or has left UM and the information is not available elsewhere, or in other situations in which it is necessary if the ordinary business of UM is to proceed. In more complicated situations--where, for example, a supervisor believes university resources are being misused--he or she should consult with senior administrators, the Office of Human Resources, or the Office of the University Attorney.

D. Students

Students are provided email and computer accounts for use primarily in connection with their academic activities. While UM does not generally monitor or access the contents of a student's email or computer accounts, it reserves the right to do so. However, access to and disclosure of a student's email messages and the contents of his or her computer accounts may only be authorized by any one of the Dean of Students or his/her designate, the Vice Chancellor for Student Affairs, the Chief Information Officer, or the IT Security Coordinator, in consultation with the Office of the University Attorney.

E. Multiple Affiliation

Some individuals have multiple affiliations (e.g., students employed by the UM). When the need for access to information arises from a particular status, the provisions above for that status will be applied. In other cases, the provisions for the individual's primary status will be applied.

III. Violations of this Policy

Members of the UM community who believe that this policy has been violated with respect to their privacy should attempt initially to resolve the issue within their unit or department, if necessary with the mediation of the leadership of their representative assembly. Others who become aware of violations of this policy should report them to the IT Security Coordinator, Office of the University Attorney, Office of Human Resources or the Office of Audit and Compliance. All University offices that substantiate such violations should report them to the IT Security Coordinator, who will monitor them for repeat instances and patterns. Those who violate this policy may be subject to disciplinary procedures, consistent with those outlined in the Appropriate Use Policy and the Information Confidentiality/Security Policy, up to and including dismissal.

Appendix 1: Special Note on Email Privacy

Email is not appropriate for communicating confidential information. Further, it is not possible to assure the privacy of email correspondence. There are a number of ways that plain text email may be disclosed to individuals other than the addressee, including:

- Recipient's address is mistyped; message is sent to someone else.
- Recipient forwards email to someone else.
- Intruders break into email system and read/disclose messages.
- Despite owner's belief that s/he deleted it, email continues to exist on computer hard drive or a copy is archived on tape backup; disclosure of such copies may be required in connection with judicial or administrative proceedings or government investigations.
- Email is observed as it travels over public networks and the Internet.
- Some virus variants will randomly send existing email messages to numerous users within an address book.

Please be aware that “Secure Document Exchange” is available myOleMiss (my.olemiss.edu) and can be used as an alternative to email to exchange sensitive documents using a secure Web interface. Likewise, UM has contracted with Box for file storage in the cloud. UM Box may be used to store certain classes of confidential information as defined in the Information

Confidentiality/Security Policy. See http://www.olemiss.edu/helpdesk/faq.php?cat=49 for more information.