The University of Mississippi

IT APPROPRIATE USE POLICY

Summary/Purpose: This policy sets forth the privileges of and restrictions on students, faculty, staff, and other users with respect to the computing and telecommunications systems offered by the University of Mississippi (UM). This is not limited to desktop/laptop systems, hand-held/mobile computers, lab facilities, centralized servers, classroom technology, the wired and wireless campus networks, cloud-based services, etc. This policy defines and gives examples of various sorts of activities which are detrimental to the welfare of the overall community and which are therefore prohibited. It also describes the process by which violators are identified, investigated, and disciplined. It should be noted that certain legal activities are in violation of this policy and are prohibited with respect to University computing and network systems. This policy is designed to protect the University community from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate use exposes the University to risks, including virus attacks, compromise of network systems and services, legal issues, and possible financial penalties. This policy directly addresses copyright issues related to illegal downloads and peer-to-peer file sharing.

PLEDGE TO STUDENTS, FACULTY AND STAFF

The University of Mississippi is committed to maintaining its leadership position in the use of computer and communication technologies to facilitate learning. The University promises to provide, as rapidly and as economically as is feasible, the following:

- **to students,** access to their information anywhere on campus.
- **to faculty,** the resources necessary to enhance teaching, learning and research.
- **to staff,** the tools necessary for a responsive service environment.

The University will normally respect privacy and attempt to safeguard information but cannot guarantee these privileges absolutely: **the University can examine, at any time, anything that is stored on or transmitted by University-owned equipment.**

The University reserves the right to limit access to its networks when applicable university policies or codes, contractual obligations, or state or federal laws are violated but does not monitor or generally restrict the content of material transported across those networks.

The University reserves the right to remove or limit access to material posted on university-owned computers when applicable university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on university-owned computers.

RESPONSIBLE USE OF EMAIL AND OTHER ELECTRONIC COLLABORATION MEDIUMS

UM recognizes the utilization of electronic communications as an efficient and necessary method of conducting business and advancing its mission of creating and disseminating knowledge. Electronic mail (email) and electronic collaboration tools such as instant messaging and chat solutions should be used with the same care and discretion as any other type of official university communication.

Principal Priorities of Email:

1. Official UM email correspondence must originate from a UM email account

patched systems are vulnerable to attack from outside entities and may be used as platforms to propagate spam, computer virus and worm’s to other hosts both on the campus and abroad resulting in loss of bandwidth and possible restrictions to other computer systems; accordingly, compromised systems will be disconnected from the campus network as soon as they are detected.

YOU MUST TAKE FULL RESPONSIBILITY FOR WHAT YOU PUBLISH, TRANSMIT, OR POSSESS.

PENALTIES

If you are suspected of violating this Policy, the University may impound any equipment, device, software, documents, or data that is involved. A search warrant will be obtained before impounding items not owned by the University.

If you have violated the Policy, you will incur the same types of disciplinary measures as violations of other University policies. Violation of state or federal free/ore/oureiplercomicinar i iplllopaeaurcons

- An individual observes what is perceived to be a violation. The office to be notified is determined by the status of the suspected violator:
    - Students: Suspicious activities should be reported to the Dean of Students.
    - Faculty: Suspicious activities should be reported to the Provost.
    - Staff: Suspicious activities should be reported to the Vice Chancellor for Administration and Finance. [Minor infractions by any account holder may be reported directly to the Complaints Committee (complaint@olemiss.edu).]

The Complaints Committee accepts reports of minor infractions (anything which is not serious and which should be correctable by pointing out the infraction to the offender, e.g., a business card on a web page) and attempts to resolve them within seven business days. If not resolved, the violator is reported through the IT Security Coordinator to his or her administrative office for stronger action. The systems administrator of a compromised system is free at any time to take immediate action to safeguard the University's infrastructure, including working with campus security to obtain a search warrant at the first sign of suspicious activity. IT personnel will also document the actions taken from the point of discovery and will prepare a non-technical narrative for the use of the University. The CIO or designee may authorize monitoring of systems to gather information on any activity that is using University-owned equipment or services. These activities will be logged by the systems administrator when undertaken and will be conducted in an appropriate manner approved by the IT Security Coordinator and the CIO.

Incidents will be reported by the systems administrator to the IT Security Coordinator, possibly the Complaints Committee, and, in addition, to the appropriate disciplinary office(s) (Dean of Students, Provost, or Vice Chancellor of Finance & Administration). These units will authorize such additional steps as may be necessary to collect evidence, including the execution of a search warrant, and setting the scope and duration of the investigation. The Complaints Committee and the IT Security Coordinator will work with the disciplinary office to decide when to notify the individuals involved that they are under investigation. If non-University service providers are involved, they will consult with the University Attorney and the CIO to notify them as soon as it is prudent to do so.

The collected evidence and the documents that record the actions of the systems administrator, IT staff, and the Complaints Committee will be forwarded to the disciplinary office for adjudication together with a recommendation on any loss of privileges with respect to computing and telecommunications systems. The disciplinary office will report the outcome of the case to the IT Security Coordinator and to the CIO. In the case of suspected criminal violations, the University Police will be involved.

The accused has the right to petition the disciplinary office for the release of impounded material and the restoration of privileges. That decision may or may not precede the disposition of the case. In any event, any such decision must be communicated to the IT Security Coordinator and the systems administrator. Faculty and staff members against whom disciplinary action is taken may follow the prescribed methods for the resolution of work-related conflicts, including the filing of a grievance.

APPLICABLE MISSISSIPPI LAWS

The following are examples of violations of the laws of the State of Mississippi (Mississippi Code of 1972 - http://www.lexisnexis.com/hottopics/mscode/ (97/045/0011)

- Public display of sexually oriented materials in a venue likely to be visited by minors in the normal course of business. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/005/0029)
- Intentional deceit of anyone as to your true identity for the purpose of obtaining anything of value. You should not use someone else's email account at all, but to do so for personal gain is illegal. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/019/0085)
- Profane or indecent language in a public place. A web page which resides on a University server is a public place. (Reference http://www.lexisnexis.com/hottopics/mscode/ (97/029/0047)
- Publishing or exhibiting obscene materials. (Reference http://www.lexisnexis.com/hottopics/mscode/ (97/029/0101)
- Hacking or passing along hacker information concerning a computer, computer system, or network to another person. Obtaining services to which you are not entitled and either inserting or changing system files are all illegal. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045/0003)
- Blocking another user from using a system he/she is entitled to use. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045/0005)
- Using or sharing the results of cracking a password file. This may result in up to five years in jail and a fine of up to $10,000. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045/0005)
- Intentional modification or destruction of computer equipment or supplies. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045/0007)
- Erasing, modifying, sharing, or using the information in the files of another user. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045/0009)
- All of the activities outlined in the Mississippi Code are unlawful if the user was physically in Mississippi when the act was committed, was committing the act against a computer or system in Mississippi, or used a computer or network in Mississippi as a relay point. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045/0011)