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 includes desktop systems, hand-held 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, and legal issues. 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

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) 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 on the UM Mail (Office 365) servers or a registered, on-campus, departmental email server. Exceptions include email to support instructional activities, which may originate from UM Gmail, and extenuating circumstances where access to UM email accounts is limited.
2. Official UM email correspondence must be concise, professional, and free of personal expressions inappropriate for a business or academic environment.
3. Email communications must not be unethical, fraudulent, harassing, obscene, or perceived to be a conflict of interest or contain sensitive/confidential information (i.e. credit card numbers, social security numbers, etc.)
4. File attachments sent via email must be scanned using current anti-virus software prior to sending the transmission. Any file attachment that is received must be scanned prior to opening the file.
5. Users must not allow anyone else to send email using their accounts.

UNIVERSITY-OWNED computer and network resources, including Internet connections and bandwidth, exist to advance the mission of the University. The University will manage these resources accordingly. Technologies such as Internet2 are provided for specific purposes. The primary goals of Internet2 are to create a leading edge network capability for the national research community, to enable revolutionary Internet applications, and to ensure the rapid transfer of new network services and applications to the broader Internet community (see internet2.edu). The University authorizes the IT to create and enforce appropriate management policies that are supportive of the goals of these technologies.

> *Examples*: The University reserves the right to send official notices to all student/faculty/staff email accounts. Campus webmasters should use discretion when linking to non-University websites. You may not install software on University-owned computers that interferes with day-to-day work or hinders the professional operation of University computers or networks. You may not set up a networked server on campus that results in the monopolization of network bandwidth or interferes with access to online academic resources.

Technology provided to you by the University is for completing work efficiently and effectively and should not be shared except for university-related purposes. Any personal use, intentional or unintentional, that incurs a cost to the University must be reimbursed.

Visitors to the university may use wired and wireless networks and technology configured for public access as long as they follow this IT Appropriate Use Policy. University employees may authorize their guests to use the wireless network. In these instances, the employee who authorizes the access is responsible for the actions of the guest.

Individual departments may place additional restrictions on personal use of the resources by their employees.

YOU MAY NOT use personal email accounts to conduct official UM business.

> *Examples*: Personal email accounts include, but are not limited to, accounts such as username@gmail.com, username@hotmail.com, username@yahoo.com, etc.

The University recognizes that there may be extenuating circumstances where communication is required but access to UM email accounts is limited, e.g., emergencies. In these cases, employees are encouraged to be resourceful in accomplishing their work and always mindful of related security issues.

PROVISIONS

You are entitled only to one person's fair share of University resources unless written permission to the contrary has been granted by the Chief Information Officer (CIO). See http://www.olemiss.edu/depts/it/policy/ for other technology-related policies.

The following list includes examples of prohibited activities, not everything that is a violation:

YOU MAY NOT use the University computing or telecommunications systems to violate copyright law. Copyright law limits the right of a user to copy, download, distribute, edit, or transmit electronically another's intellectual property, including written materials, images, videos, software, games, sounds, music, and performances, even in an educational context without permission. Violations of copyright law may include giving others unauthorized access to copyrighted materials by posting that material on social networking sites, downloading from Internet websites or through peer-to-peer (P2P) file sharing any material owned by another without the owner's permission, or sharing files that include copyrighted material with others through peer-to-peer software or networks. Peer-to-peer is a method of file sharing that allows normal users ("peers") to connect directly to other users to share files. This can be contrasted with a server-based distribution method, where users connect to a server (such as a web server via their web browser) to download files. If you have P2P file-sharing applications installed on your computer, you may be sharing copyrighted works without even realizing it. Even if you do not intend to engage in infringing activity, installing P2P software on a computer can easily result in you unintentionally sharing files (copyrighted music or even sensitive documents) with other P2P users, and you may then be personally responsible for the legal and financial consequences.

> *Examples*: You use a file-sharing program or client, like BitTorrent, Gnutella, and LimeWire, Kazaa, BearShare, or others, to download or distribute movies, songs, games or software without authorization from the copyright owner. RIAA (Recording Industry of America) and MPAA (Motion Picture Association of America) can and do aggressively look for these violations. Alternatively, if you join iTunes and purchase several songs to play on your iPod, this is not a violation of copyright law.

In addition to the penalties outlined elsewhere in this policy, infringement of copyrighted work,

including unauthorized P2P file sharing, may also involve civil lawsuits by the copyright owner. Possible penalties include actual damages and profits or statutory damages of up to $30,000 for each work infringed (or up to $150,000 for each willful infringement), court costs, attorney fees, and other civil damages. Criminal penalties for willful infringement may include, depending upon the value of the work(s) infringed, fines and imprisonment for up to 3 years as provided in 18 USC 2319.

Please be aware that there are many legal alternatives for downloading media such as iTunes, Pandora, NetFlix, and Amazon MP3. A list of popular, legal, fee-based and free alternatives is available to you at: http://www.educause.edu/legalcontent.

See the Higher Education Opportunity Act (HEOA) (http://www2.ed.gov/policy/highered/leg/hea08/index.html) and related federal regulations at 34 C.F.R. §§ 668.14 (b)(30) & 668.43(a)(10) for other copyright-related requirements for US colleges and universities.

YOU MAY NOT steal, forge, lie or cheat with; snoop on; tamper with; misuse, damage, harass with; threaten with; hoard or monopolize; interfere with; violate the confidentiality of; masquerade with; or destroy any information, resource, equipment or software. This includes using your personal computer for these activities against other users or against their information resources.

> *Examples*: You must not access the account of another; you must not generate activities which consume more than your share of either system time or network bandwidth (including chain letters); you must not fraudulently log into any computer, etc. (Reference: http://www.lexisnexis.com/hottopics/mscode/ (97/045) You must not upload, post, or transmit content that is threatening, harassing, defamatory, libelous, invasive of another's privacy. This includes but is not limited to social networking sites, blogs, email or other electronic correspondence. You must not forge email headers or manipulate other identifiers in order to disguise the origin of any system or network activity.

YOU MAY NOT possess any software, resource, or equipment whose purpose is to effect one of the violations listed in the previous Provision nor may you attempt to violate the previous Provision. Any such attempt will be considered to be the same as a violation.

> *Example*: You must not have in your account on any University-owned system or on your personal computer programs that attempt to determine the passwords of others or obtain privileges on any computer to which you are not entitled. If you attempt to obtain system privileges to which you are not entitled, you are as guilty as if you had succeeded.

YOU MAY NOT possess, willingly receive, or distribute obscene material.

> *Examples*: Child pornography is absolutely against the law. It is a violation of Federal law to transmit this material across state lines, even electronically, and certain obscene materials are in violation of the Mississippi Code. (References: http://www.lexisnexis.com/hottopics/mscode/ (97/005/0029) and http://www.lexisnexis.com/hottopics/mscode/ (97/029/0101)

YOU MAY NOT violate the IT Appropriate Use Policy off-campus anywhere in the world using University resources.

> *Example*: An attempt to gain unauthorized entry to any computer off the University campus is as if you attempted to gain access to a computer here.

YOU MAY NOT use any University facility for non-University commercial business or advertising, including unsolicited commercial email without written permission from the Provost and the CIO. This includes partisan political activities; however, any officially sanctioned University student group may maintain an official Web page which presents objective information about the group itself. Commercial sponsorship of academic projects, e.g., the inclusion of banner ads on project web sites, is allowed in certain cases. These requests must be approved by the CIO.

> *Examples*: You may not use the statistics software on the academic shared systems to do work for off- campus entities for which you are paid. The Young Democrats/Republicans may have a page that presents information about their activities and goals; they may not attempt to influence voters' choices through that page. The sending of unsolicited bulk email (spamming) is not allowed when it is unrelated to the University's mission.

YOU MUST connect all equipment and install all software in a manner that meets the technical, security and fair use standards set by the Office of Information Technology (IT).

> *Examples*: All IP addresses and domain names are owned and assigned by the IT as specified in the UM Policy for Domain Name Registration . World Wide Web, ftp, and other network services that interfere with fair network use by others may be restricted by the IT. You must follow proper use guidelines when using classroom technology, e.g., powering down projectors according to vendor specifications. Improperly secured and 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/statutes may lead to

criminal or civil prosecution.

Students: Campus disciplinary measures may include, but are not limited to, failure in a class, permanent or temporary loss of information technology privileges, suspension or expulsion from the University, and restitution of expenses as well as charges for damages.

Faculty and Staff: Campus disciplinary measures may include, but are not limited to, reassignment of duties, transfer, censure, suspension, termination, and restitution of expenses as well as charges for damages.

Off-campus Users: The University may revoke the privileges of users who are found to be in violation and may report any serious violation to the users home campus authorities and to appropriate law enforcement officials.

INVESTIGATION AND DISCIPLINARY ACTION

Violations are most likely to be observed in two ways:

- A system administrator detects an anomaly and, in determining the cause of the problem, finds evidence of a violation.

  Caution: In exceptional cases, a system or network administrator may detect evidence of a violation while performing his or her duties operating or maintaining a system. In these instances the priorities of protecting the University against seriously damaging consequences and/or safeguarding the integrity of computers, networks, and data either at the University or elsewhere, may make it imperative that the systems administrator take temporary restrictive action immediately. In these instances, all restrictive actions taken must be documented and justified in accordance with this policy. The Complaint Committee and/or IT Security Coordinator must be immediately contacted so the complaint can be further investigated and processed.

- 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 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)