Personnel Directory
Information Technology

Desktop & Office
Hardware
Software
Telephone

Campus Systems
Banner
Email & SPAM
FlightPath
Kaltura Capture
Moodle
myULM Portal
VPN
Web Programming
Wireless / WiFi
ZOOM/Video Conferencing

Computer Labs
VR Classroom/Lab
Open-Access Labs
Lab Software Request
Sandel 211 Video Conference Room Request

Policies & Forms
Technology Use Policy
Other Policies
Forms Database

Contact:
Office of Information Technology
University Library
Room 302, ULM
(318) 342-5015
FAX (318) 342-5018

Technology Acceptable Use Policy

Information Technology

University of Louisiana at Monroe Acceptable Use Policies

NOTE: The University of Louisiana System is compiling an acceptable use policy to govern all universities under its jurisdiction. This policy will be modified as needed to meet the requirements from the Systems Office.

ULM faculty, staff and students who use the computing resources must be sensitive to issues pertaining to system security and confidentiality of information. With ULM's connection to the Internet, the need for security awareness has increased more than ever. With greater availability comes added responsibility. Not only can a user of the ULM systems access local data but, via networks, data and systems throughout the world. Anyone accessing these systems is responsible to the University and to other users to make legal and proper use of these facilities. Only properly authorized persons may access network or computer facilities. Proper authorization is given to users in two forms:

- Assignment of an account, "id" or "sign on" issued in the name of the authorized person by Information Technology or an area responsible for departmental services
- Access to lab services not requiring a computer "id" but nonetheless bound by the requirement of legal and proper use

The person requesting an account is required to complete and sign the Application for Accounts form, affirming that the applicant understands and will comply with the listed policies. By applying for and using an account on University computer systems, a person agrees to abide by the following statements:

- I will use the ULM facilities for University business only.
- I will not allow other persons to use my account and acknowledge that providing other persons with access in such a manner is considered a serious violation of my obligations.
- I understand that I have an obligation to protect University hardware, software, and data. I will not attempt to gain access to accounts, data or systems for which I have no authorization.
- I understand the University is co-owner of all files on the system and has all rights to those files.
- I understand that any violation of these terms and conditions, abuse of equipment, breach of security or use of systems to intimidate or harass others will result in loss of privilege to use the system and that serious offenses will result in more serious disciplinary action.

These statements are listed on the Application for Accounts and are applicable to all computer resources at the University. Student accounts are automatically generated without the requirement of this form; however, students are still to be aware of and abide by this policy; listed in the Student Handbook. Users are responsible for all activities that occur through an account that has been issued to them. If you believe that another party has compromised the account, you should report your suspicions to Information Technology staff immediately.

CONFIDENTIALITY OF INFORMATION

It is important that all users understand that the University is co-owner of all file(s) on University centrally supported computer systems, networks and all PC's and accordingly has all rights to its files. From time to time, it may be necessary for Information Technology staff to access individual user file(s) while providing system maintenance or individual user support. We will make every effort to minimize this type of access, but due to the nature of our services, it is inevitable that some access of this type will be required. Due to the nature of an individual's work assignment and the information which is stored on ULM computer systems, employees (faculty, staff, and student workers) may have access to information which is private and confidential in nature, i.e., grades, financial information, payroll information, etc. It is the responsibility of people who have access to this type of data not to disclose this information except for on a "need to know" basis. Furthermore; all possible precautions should be made to insure that any sharing of data is accomplished within the guidelines of all pertinent laws and regulations, such as the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley (GLB) Act. It is the shared responsibility of the Information Technology staff and the department that "owns" the system to insure that the data which are stored on University systems is treated with the appropriate level of privacy and confidentiality. Information Technology will provide the electronic access security which is required for these systems and the head of the department that owns the system (or their designee) will determine who is issued what level of access. For example, the Registrar will determine who can have access to student information; the Controller will determine who has access to financial information, etc.

Ethical behavior

With the privilege of access to the ULM systems, comes a degree of standards for ethical interaction. Some unacceptable uses, but not limited to, are as follows:

- Participating in activities which use excessive data storage or network bandwidth. Initiation or propagation of chain letters or mass e-mails (spamming) that substantially disrupt ULM systems are not acceptable. Continual use of Internet based radio and or access to video feeds are a drain on bandwidth and therefore not appropriate.
- Sending harassing or threatening e-mail.
- Intentionally introducing, creating, or propagating disruptive code into the system (worms, viruses, Trojans, etc.)

- Interfering with another user's legitimate use of services.
- Use University computer resources for personal profit, except as permitted under the ULS Policy Number: FS.VII.-1, Outside Employment/Procedures.

Copyright

Users are responsible for abiding by copyright laws and licensing agreements in the use of electronic media via University equipment or networks. Unauthorized access or copying of proprietary data (such as programs) is forbidden and subject to civil and criminal penalties for violation of federal copyright laws.
Prohibited activities include, but are not limited to the following:

- Installation of non-approved software and computer piracy are prohibited.
- Unauthorized distribution of copyrighted material
- Unauthorized peer-to-peer file sharing

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq

SYSTEM SECURITY

It is also the responsibility of the department that owns the system to ensure that adequate procedures are in place to insure that these security and control measures are implemented appropriately. Each user must have his/her own individual account and users should not share accounts or give their passwords to others, particularly if that account has significant authority to access highly confidential information or power to update. Passwords should be kept confidential and not taped to the terminal or PC. Users should not stay logged on to a system when they will be leaving their device for a period of time. If a user is accessing confidential information and is required to walk away from their device even for a short period, they should clear their screen, especially if that device is in an area that is generally accessible. Information Technology provides software-based security that is installed to protect the integrity of the user accounts, programs and data. However, the matter of security must be of concern to users at all levels, from supervisory to support personnel. Each user of the University's equipment and networks must exercise the appropriate responsibility and caution to assure that security is maintained.

SECURITY TIPS

Following these few simple guidelines will help to insure the integrity of University computer systems.

- Memorize your password(s). Do not write passwords down and post in easy to find locations. If you must write your password down, do so in a discrete manner and keep in a secure location not associated with your terminal.
- Do NOT use e-mail as a means of sending Personally Identifiable Information (PII) of any individual. PII is any combination of Name, CWID, SSN, Grades, Birthdate, Address, etc. E-mail does not guarantee privacy and confidentiality of information and is therefore not a secure means of data transmission for PII. Use of departmental fileshares is the ULM recommendation for those offices that need to share PII related content.
- Do not tell anyone your password. If someone needs access to your device, (ex. to verify that it works) log on for them. If you ever receive a call from someone claiming to be from Information Technology, who asks for your access code in order to verify something, require them to come to your office and verify the process in your presence.
- If an unfamiliar person wants to use your device, be certain to verify their identity and whether they have authority to use the system. If you are currently logged on to a system, log off before allowing them on.
- Do not leave your device unattended and logged on in an area available to unauthorized users. If you must leave for an extended period and there is a chance someone can access your device who should not, log off.
- If you suspect that someone knows your password, set a new one before your data can be compromised.
- Change your password on a regular basis.
- All security violations, intentional or otherwise will be taken seriously.

INB Password Policy:
When granted a Banner INB account, upon first login, you will be required to change the issued password before proceeding. The requirements for the password is a minimum of 6 characters, the only character that is not allowed is "@". After setting your new password, you will be required to change the password every 90 days and you cannot reuse a password for a minimum of 365 days. The system also gives a grace period warning before the current password expires.

Disclaimer

The University of Louisiana at Monroe is subject to a hierarchy of governing bodies. The Office of Information Technology for the State of Louisiana is working on a draft 'Acceptable Internet/E-mail Use' policy. Upon acceptance of such a policy, or such from any other of the bodies superior to the University, statements within this policy may be superseded.