

Document III

UL LAFAYETTE COMPUTER & NETWORK POLICY

Purpose & Scope

This document sets forth the University's policy with regard to access to and use of computing and network resources by faculty, staff, or students. It is intended to apply to any computing or network resource owned, operated, or otherwise provided to users by the University of Louisiana at Lafayette. (It does not apply to the use of facilities owned and operated by commercial Internet service providers, even those who offer discounts to members of the UL Lafayette community, but some of the advice provided in this document may be appropriate on any facility.)

Computer and network users at UL Lafayette are responsible for knowing this information on the proper, ethical, and legal use of computing and network resources provided by the University.

This policy does not preclude enforcement under the laws and regulations of federal, state and local authorities.

The University reserves the right to change this policy in response to altered or unanticipated circumstances.

Any questions concerning computing or network policies at UL Lafayette which are not resolved by this document should be directed to the Vice President for Information Technology.

Authorized Access

Only persons properly authorized may access UL Lafayette's network or computer facilities. Proper authorization is provided by authorized staff in the form of an "account" issued in the name of the authorized person. Accounts are only issued to individuals, not to organizations, departments, or other groups of people.

All faculty, staff, and students are eligible for e-mail accounts; however their data must be correctly entered into the administrative database before their account can be issued, as computer support staff depend upon the administrative database to verify initial eligibility for an account, to obtain a unique, permanent ID for a user, and to learn of any change of status which signals that an account should be removed.

Departments which desire to assure new or visiting faculty of e-mail accounts prior to the beginning of the semester should send appointment letters to the Business Office with a note requesting early entry into the database so that e-mail accounts can be established. Individual faculty, staff, or students must take responsibility for verifying that they are correctly represented in the database and for obtaining any needed corrections through the appropriate administrative office.

Removal of a person from the administrative database will result in termination of the account. Typically such removals result from: employees who resign or are terminated; or students who fail to register for the fall or spring semesters.

Short term accounts may be authorized to meet particular needs. These normally require a faculty/staff sponsor to be responsible for use under the temporary account and require approval through the sponsor's vice president. Contact your system administrator in advance to discuss required procedures.

The University does not provide accounts to Alumni.

Policy on Computer Accounts and Access to Administrative Systems

ID Creation

Common Logon Identification (CLID) and associated passwords for the IBM mainframe are distributed to University personnel on a business need. There is currently no business need for students to directly use the IBM mainframe. The CLID is generated, revoked, and restricted based upon the presence of credentials occurring in the official University personnel file. A person who has credentials in the personnel file may obtain a CLID and password for the IBM mainframe by filling out an MVS ID request form and having it signed by his or her supervisor. The person may also need approval for access to data from the department responsible for the data. If a person transfers between budgetary departments the CLID will be restricted and he/she will have to prove need-to-know by filling out a new MVS ID request form with appropriate signed approvals.

ID Revocation

CLIDs are revoked for the IBM mainframe when the person no longer has current credentials in the personnel file (i.e. resigned, terminated, retired). Revocation means removal from all IBM accounts and privileges, i.e. login (TSO, IDMSPL, IDMSPL, IDMSPL), and access to screens (IDMSPL, IDMSPL, IDMSPL). Revocations are done on a weekly basis or immediately upon request.

Restriction

Restriction occurs when the person transfers from one budgetary department to a different budgetary department. Restriction implies that the person will retain limited access and privileges, i.e. login (IDMSPL) and inquiry access only to screens (IDMSPL). All add, change and delete access will be removed. Need-to-know access for the new department will have to be approved by submitting a new MVS ID request form with appropriate signed approvals.

Authorized Activities

UL Lafayette provides computing and network resources to faculty, staff, and students, at University expense, primarily for their use in administrative or academic pursuits and secondarily for any personal exploration and enrichment which does not conflict with the primary purpose of these resources or with any applicable law or policy.

Historically, available computational resources at UL Lafayette have not adequately handled all of the various needs. Thus, prudent utilization of available resources is a necessity. Policies described in this document seek to facilitate usage directly related to the academic and administrative missions of the University, limit optional use to times when no primary uses will be adversely affected, and eliminate illegal or abusive usage. In addition, policies are included to help maintain an ethical and amicable working environment for all computer and network users.

Usage that results in specific, substantiated complaints from another user will result in a re-evaluation of that activity.

By University policy, gaming is not authorized unless it is an official class assignment.

By State law, any personal for-profit activity or any activity which competes with local business is prohibited.

Use of UL Lafayette's computing facilities on behalf of any organization, even non-profit organizations or UL Lafayette-affiliated organizations, requires prior approval by the UL Lafayette administration.

If you are uncertain whether a specific activity is acceptable, discuss your concerns with a system administrator or with the Vice President for Information Technology.

Other Usage Issues

Priority

Those computing or network applications which enable students, staff, and faculty to meet the recognized educational, research, and administrative goals of the University have priority.

No use should interfere with the use of UL Lafayette systems as a tool to accomplish academic or administrative work at the University. Secondary use of scarce resources should be minimized or deferred until times when they will not interfere with the primary functions of the resources. Examples of scarce resources are UCS Sun workstations during peak usage; or dialup ports at most times.

Other uses are proper only if the resources are not otherwise needed, and the use is not prohibited by other applicable policy, i.e. University, School, Department, or system administrators of the facilities you want to use. In determining whether your proposed activities will adversely affect other users consider network traffic and restrictions on simultaneous use of any resource (e.g., ports or licenses) as well as competition for the particular system(s) you want to use. If your non-primary use will inconvenience any user working on a primary mission (administrative or academic) application, whether by delayed response times or any other factor, then your use should be deferred until later.

Integrity

Users are presumed to be responsible for all use and any charges pertaining to their account. Do not allow anyone else to use your account. (If you need to share files, there are other ways to do so: contact your system administrator for assistance.)

Users who make deliberate attempts to hide their identities from other users or system administrators are in violation of University policy (e.g. sending e-mail with headers deliberately altered to hide the senders identity).

Users may be required to show UL Lafayette ID cards to obtain access to computing and network facilities or to pick up printouts. Printouts will only be given to the user whose UL Lafayette ID card matches the account information on the printout, unless other distribution arrangements have been approved by the system administrator.

Users who attempt to crash or subvert security or otherwise adversely affect operations on any system are in violation of University policy and possibly in violation of various laws.

Keep your password secret and change it from time to time. If you believe someone has guessed your password, you should change your password immediately and report this problem promptly to the system administrator. Failure to do so will make you accountable for any (mis)use of your account.

Conduct

Users may not harass or threaten other users, attempt to steal passwords, files, or other user/system information, attempt to crash, violate the integrity of, or adversely affect the activities of a computer system or network. Distasteful or offensive displays, messages and printouts are not permitted. Actions which adversely affect the working environment of other users are unacceptable. Music, playback of sound files, or loud conversations are not suitable in a shared lab environment. Physical abuse, mishandling and modification of terminals, printers and other hardware is not permitted.

Waste

When any process is consuming excessive system resources or objectionably degrading system response it may be terminated, or its priority may be altered, without notice. Unnecessary storage of

disk files, careless execution of high resource consuming programs, or generation of excessive printed output is wasteful. Users should also be aware that hard copy output devices are expensive to operate and that wasteful usage of such devices may result in charges to the account that requested the output. Sending "chain letters" or unwanted e-mail to a large number recipients ("junk mail") is wasteful and inappropriate.

Storage Space

Users are responsible for managing their disk storage allocations. When users exceed their disk storage allocation, they are notified. Some systems notify users by electronic mail or direct message. If the storage allocation is exceeded for an extended period, the user account may automatically be disabled. Computer files not related to official missions of the University and which consume large amounts of space may be removed without warning by system administrators in those cases where they impact system operation.

Electronic Publication

Posting to an Internet discussion group or displaying personal web pages are a form of publication and because electronic publications can be created so easily, the checks and balances that help produce responsibility in print media may not operate until it is too late.

Users are responsible for the content and the consequences of their electronic publications. Various local, state, and federal laws (such as but not limited to: copyright, obscenity, libel) may apply, as may the laws of other jurisdictions and countries. What is acceptable may also depend on your intended audience, or whether your publication can be accessed by minors.

Because anything you place on the Internet from UL Lafayette can easily be determined to have originated on a computer connected to the UL Lafayette network, some of your readers may assume that your publication is somehow sponsored by the University. Unless you have such authority, you should include a disclaimer on your publication. This can be quite simple and informal, for example: "I speak for myself, not for UL Lafayette." (Such disclaimers are very common on the Internet and may be included in .signature files.) Do not use official UL Lafayette logos or seals unless you are specifically authorized to do so.

If you expect to publish something that will attract a great deal of attention from other people on the Internet, you should discuss it with your system administrator first. It is possible for the reactions from the net to overburden the system you use or the campus link to the Internet.

Licenses and Contracts

The University normally acquires hardware, software, and other services under educational agreements which often restrict the use of the item in some way. For example, some items may not be used to develop administrative applications or may be restricted to certain groups of users. Exclusion of any commercial use is typical. Other licenses may limit who can examine the source code or the documentation. Licenses also place limits on the number of simultaneous users or the number of or location of systems on which the software can be installed. Normally, it is legal to copy a software product only for backup purposes -- that is, for recovery from system or disk failure.

Unless you have a specific, written statement from the vendor with different provisions, assume that a single educational license can be used on only one University-owned CPU at a time. Violating software licenses provisions can result in very substantial (\$100,000) personal liability.

Faculty or staff who foster innovative, co-operative agreements with any off-campus group should consult with system administrators for license or other restrictions.

Privacy

Although system administrators are co-owners of all user files, the University recognizes that faculty, staff, and students have a substantial interest in privacy with regard to their computing activities, even when those activities involve only University business.

Monitoring

The University will not monitor user transactions or the contents of user files as a routine matter. It will respond to legal process. It may inspect without notice the contents of files in the course of an investigation triggered by indications of impropriety or as necessary to resolve system problems or to locate substantive University-related information that is not available by some less intrusive means.

It is a violation of University policy for any employee, including system administrators and supervisors, to use the computing systems to satisfy idle curiosity about the affairs of others, with no substantial purpose for obtaining access to the files or communications of others.

Grounds for examination of user files

Circumstances which may require a system administrator to inspect the contents of files created or maintained by University faculty, staff, or students are:

- a search warrant or subpoena specifically pertaining to user files, served by law enforcement authorities;
- reasons to believe that the file is connected with violations of University policy or State or Federal law;
- investigation of a specific, substantiated complaint by another user, either at the University or at another site about activities originating from a UL Lafayette user's account;
- reasons to believe the file is directly related to system errors or malfunctions;
- an urgent need, by a supervisor or project administrator, to access critical University information which is maintained by one of his/her staff or project members and which cannot be obtained by less intrusive means.

Such circumstances are reviewed by the head of the department (or his/her designee) in which the computing system is located, prior to granting access.

Users should also be aware that system administrators may accidentally view the contents of a file during routine system operations. A common example is a system postmaster seeing a portion of an e-mail message while trying to route bounced mail to the appropriate destination.

Disclosure

System administrators who obtain access to personal computer files will disclose this information only for a legitimate business need of the University or to protect the interests of the University or as required by law. Any internal disclosure of message content shall be limited to those University employees who have some reasonable need for this information.

Anyone who stores both critical University-related material and personal information is encouraged to clearly differentiate these items (using descriptive names and separate storage areas, for example) and take steps to ensure University-related documents should be available to co-workers.

Handling Problems

Problem Reports

System administrators rely on users to report policy violations or other problems that they are aware of. System administrators will need specific details to be able to investigate and/or resolve most types

of problems, so please provide all information that seems likely to be helpful, as well as a way to contact you, in case more details are needed.

Policy problems which cannot be resolved by a UL Lafayette system administrator may be referred to other appropriate University personnel, such as advisors, other department heads, deans, or campus security.

Penalties

Penalties may include loss of access, either temporary or permanent, to UL Lafayette computing systems and networks. This does not preclude enforcement under any applicable local, state, and federal laws.