OFFICE OF THE CHANCELLOR
LOUISIANA STATE UNIVERSITY AT ALEXANDRIA

Revision: 0
Effective: October 1, 2004

SUBJECT: POLICY CONCERNING TECHNICAL RESOURCES

PURPOSE: To establish policies and standards for system ownership responsibility and to ensure that each technical resource meets functional requirements, is appropriately documented, is secure and controlled, has been adequately tested, is maintainable and provides audit features.

GENERAL POLICY

The standards and policies presented herein govern data systems, infrastructure, and technology resource usage at LSU Alexandria. These standards and policies apply to all computerized systems and associated information technologies involved with the creation, updating, processing, outputting, distribution, and other uses of electronic information at LSU Alexandria. They are extracted in part from common standards at educational institutions throughout the United States, and reflect standards for security and audit ability. All specifications indicated are independent of system architecture and apply to mainframe systems, networks of computers and servers, stand-alone computers and servers, networking infrastructure and any other information technology whether developed at LSU Alexandria or acquired from external vendors. The standards apply to all applications that deal with financial, academic, administrative, or other electronic data. The policies and standards contained herein will be reviewed periodically and supplements/changes made as needed by appropriate University personnel and/or committees. The University community will be notified of such changes per the distribution procedures outlined herein.

I. Policy Interpretation and Enforcement

The Information Technology Advisory Committee (ITAC) executive committee shall be the primary contact for the interpretation, enforcement and monitoring of this policy. Any legal issues shall be referred to the LSU System Legal Office for advice.

A. Interpretation

The ITAC executive committee or designee shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

B. Enforcement
The ITAC executive committee or designee shall work with the appropriate administrative units to obtain compliance with this policy

II. User Accounts and Passwords

A. Account Eligibility
1. All full and part-time employees are eligible to receive an Active Directory account which provides them with network, email, online courses, and myLSUA access. Other types of accounts are provided on an as-needed basis and are authorized by the University official in charge of the corresponding system.
2. All students enrolled in one (1) or more hours are eligible to receive an Active Directory account which provides them with network, email, electronic courses, and myLSUA access.
3. Student accounts will be disabled four (4) months after the student's last enrolled semester.

B. Account Creation and Ownership
1. Active Directory (AD) accounts for employees are created on a manual basis. Once Information and Educational Technology (IET) Services receives notification from HRM of a new employee, an AD account is created within 24 hours of official start date or notification from Human Resource Management.
2. PowerCampus accounts are created on an as-needed basis. A PowerCampus Access Request Form originates within the employee's department. This form is routed to the Registrar for approval to the Admissions and Records Modules; and to the Director of Accounting Services for the Cash Receipts and Billing Modules. Once approved, the form is submitted to IET Services for account creation. IET Services keeps all official records of account creation.
3. PowerFaids accounts are created on an as-needed basis. A PowerFaids Access Request Form originates within the employee's department. This form is routed to the Director of Financial Aid for approval. Once approved, the form is submitted to IET Services for account creation. IET Services keeps all official records of account creation.
4. Student Active Directory accounts are created automatically daily up until the last day to drop/add at the beginning of each semester. Accounts can be manually created on an as-needed basis.
5. Each user is considered the owner of his/her associated account. All activity associated with the account is the responsibility of the owner.

C. User Responsibility and Accountability
   1. Users may not allow other individuals to use their LSUA assigned network, email, or other University based account. Employees and students are individually responsible for the proper use of their assigned accounts, and are accountable for any and all activity associated with the account including email and personal web site content.
   2. Users are also responsible for the security of their assigned accounts. Users should take proper security measures to ensure the integrity of their accounts, and should also report any notice of unauthorized access.

D. User Account Format
   1. Employees
      a. User Accounts for employees of LSUA will be formatted in one of two ways: 1) First initial followed by last name, and 2) first name followed by last initial. Exceptions to this will be made when duplicate accounts would be created. Any account created prior to this policy will remain unchanged.
   2. Students
      a. User Accounts for students of LSUA will be formatted as follows: First initial followed by the full last name followed by a three digit sequential number for duplicate accounts. Example: John Smith would be jsmith001. The second John Smith will be jsmith002, and so on. Any account created prior to this policy will remain unchanged.
   3. Department and Miscellaneous Accounts
      a. As a general rule, department accounts will be an alias created to point to an existing user account. Other arrangements such as the creation of multiple mailboxes may be made only if an alias will not completely satisfy all department email requirements.
      b. Other miscellaneous accounts will be created on an as-needed basis. Formatting for these accounts will be done according to the requirements of the account.

E. Passwords
   1. Passwords are an important aspect of computer security and provide the front line of protection for user accounts. Poorly chosen passwords may result in the compromising of the University's entire network. All university employees are responsible for selecting and securing their passwords. Each user shall observe the following password guidelines:
      a. All user ids and passwords will be unique to each authorized user.
      b. Passwords will consist of a minimum of six (6) alpha-numeric characters. Common names and/or phrases may not be used.

c. Password will be kept private. Passwords may not be shared, coded into programs, or written down.

d. Password will automatically expire after 90 days. All users will be required to change their password at this time. Student passwords are an exception. Student passwords will be reset at the beginning of each fall semester, and must be changed immediately by the student. The password will be good for one (1) year.

e. A user account will be "frozen" after five (5) failed login attempts.

f. Administrative system sessions will be suspended after sixty (60) minutes of inactivity. A password will be required to log back in.

g. Successful logons to the University administrative software should display the date, time, and location of the last successful logon.

h. User ids and passwords within the University administrative software will be suspended after 30 days of inactivity.

IET Services will *never* ask an employee for his/her password. Employees should never give out their password to anyone – this includes other employees in the same office/department, and/or any outside vendor.

F. Account Expiration and Deletion

1. Employee User Accounts (including, but not limited to AD, PowerCampus, PowerFaids and Docubase) will be disabled upon receipt of the HRM sign-out form when an employee separates from the university. Each month, HRM will send a complete list of separations to IET Services for review. Any accounts not disabled via the sign-out form will be disabled once listing is received from HRM. Disabled account documentation will be stored with IET Services. Exceptions will be made only with approval of the appropriate vice-chancellor or chancellor.

   a. PowerCampus accounts are "disabled" by creating a random, complex password since the system will not allow for an accounted to be turned off. Logs are available showing last-login dates for each user.

   b. PowerFaids accounts are disabled within the software system.

2. User Accounts may be deleted from the corresponding system six (6) months after the employee's termination of employment with LSUA. Users are responsible for any personal data associated with the User Account.

3. Student User Accounts will remain active for four (4) months following the end of a semester. If a student enrolls in the following semester, the account will stay active. If the Student does not enroll in the following semester, the account and all associated data will be purged from the corresponding system.

III. Copyright, Proprietary Rights and Licenses

A. Duplication of Software

All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any University facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

B. Number of Simultaneous Users

The number and distribution of software copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

C. Copyrights

In addition to software, all other copyrighted information (text, images, icons, programs etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media. Please see LSUA Policy Statement No. 216 for additional copyright information.

IV. Network Usage and Standards

A. General Guidelines

1. The University network is defined to include any and all computer and electronic based communication facilities and/or equipment, which are owned or operated under the supervision of LSUA. The University network is for use by authorized personnel affiliated with the University, consistent with, and in the course of, their official work, study, and/or research. Individual groups or projects within the University may adopt more restrictive network usage policies that apply to their sub-networks and personnel within their area. Acceptable and unacceptable uses of LSUA network resources are outlined in the following sections. Note: These lists are not all inclusive.

B. Acceptable Uses

1. Any use that is necessary to complete research and/or coursework as assigned by or to any university employee or student.
2. Communication for professional development or to collaborate in research and education.
3. As a means for authorized users to have legitimate access to remote facilities such as email, network resources, and/or Internet access.
4. The publication of information via the Internet's World Wide Web (WWW), File Transfer Protocol (FTP), or similar techniques.
5. Other administrative and/or academic communications or activities in direct support of University projects and missions.
6. Incidental personal use may be allowed when such use meets the following criteria; it does not interfere with University operations, it does not compromise the functioning of University network and computing resources, it does not interfere with the user's employment or other obligations to the University, and it does not violate any other University policy.

C. Unacceptable Uses

1. Any use deemed commercial or for-profit.
2. Any use that is likely, intended, or by negligence causes unauthorized network disruption, system failure, or data corruption.
3. Any use related to achieving, enabling, or hiding unauthorized access to network resources, University owned software, or other information belonging to the University, either within or outside the University network.
4. Any use related to sending/receiving electronic mail that includes, but is not limited to, the following: solicitation or commercial use, forging any portion of an electronic mail message, spamming (bulk unsolicited email), or sending unwanted messages to unwilling recipients.
5. Intentionally circumventing or building an unauthorized conduit through the University firewall with intentions of bypassing University network management and security devices.
6. Use of another individual's identification; network, email or other university based account; and/or related passwords.
7. Unauthorized transfer or entry into a file to read, use, or change the contents; or for any other reason.
8. Use of computing facilities or network resources to send obscene, harassing, abusive, or threatening messages or computer viruses or worms.
9. Any use that violates University policies, procedures, and contractual agreements.
10. Any use that violates local, state, or federal laws.

V. Email

In general, use of University email services is governed by policies that apply to the use of all University computing and networking facilities as outlined in this document. The following sections are more specific to email usage and restrictions.

A. Account Eligibility
   1. All employees and students that are assigned an Active Directory account as outlined within this document will receive an email address with the same name.

B. Purpose of Email Services
   1. The University provides an email account to every employee and student of the University for the purposes of teaching and learning, research, administration and community service.
   2. The University permits this account to be used for limited incidental personal purposes. However, it is most concerned to ensure that the account is used as effectively as possible in support of the above purposes and to facilitate the work of the University. A University email account may not be used for engaging in non-LSUA business or for personal gain, except if permitted by other University policies.
   3. The email address supplied by the university is considered to be the official email contact point for University staff and students, and official University email correspondence will be delivered to this address.
   4. Email accounts may also be used for the submission and return of student assignments and other specific uses, but only where the relevant Faculty or Unit has specifically authorized this.

C. Broadcast Emails
   1. Broadcast emails are defined as messages sent to the entire campus, or a very large group of users within the University.
   2. The use of broadcast emails from the University will be kept to a minimum level and will only be used for purposes of official University business.
   3. Students will not be allowed to send broadcast emails. In the event a student needs to send a campus-wide message, such requests should be handled through the Chancellor's Office or designee.

D. Regular Accessing of Emails

1. It is important for faculty and staff to access and read email messages sent to their LSUA email account on a timely basis and will be presumed to do so. Students are expected to check their official email address on a frequent and consistent basis in order to stay current with University communications and class assignments.

E. Assignment of Student Email Addresses

1. All students will be assigned an official University email address. It is to this official address that the University will send email communications; this official address will be the address listed in the University's Global Address List found in the Exchange/Outlook Address Directory.

F. Educational Uses of Email

1. Faculty may determine how email will be used in their classes. It is highly recommended that if a faculty member has email requirements and expectations, they specify these requirements in their course syllabus. Faculty may expect that students' official email addresses are being accessed and may use email for their courses accordingly.

G. Email Storage Guidelines

1. Storage space on emails servers is limited. Users should "clean up" their mailboxes on a regular basis. Messages not needed or not related to University business should be deleted.
2. All messages placed in the "Deleted Items" folder will be deleted after 14 days. All messages placed in the "Junk Mail" folder will be deleted after 7 days. Users should take necessary action to ensure messages needed for University business not be placed in either of these locations.
3. All University-based email will follow state guidelines for archival methods and procedures.

VI. Telephone Services

A. General Guidelines

1. Departments are responsible for determining when an employee needs to have access to telephone services and the type of services necessary to fulfill University job responsibilities.

2. Personal phone calls made on University telephones should be kept to a minimum. If employees need to make a personal call which, if dialed direct, would result in a long distance phone charge to the department, they should either call collect or charge the call to their home phone or personal calling card. Personal long distance calls should not be charged to the University. If due to an emergency or inadvertence, a personal long distance call is charged to a University account, the caller will be required to reimburse the University. More than incidental personal use of a University cellular phone plan may also generate incremental costs to the University. Employees will be responsible for such incremental costs.

3. Administrative officers and supervisory personnel may establish telephone use policies that are more, but not less, restrictive than this policy.

B. Number Assignment

1. Each employee will be assigned a direct telephone number. In the event an employee only needs a local "campus only" number, this type of service will be provided. Along with a direct extension, each employee will receive a long-distance authorization code to be used for University-related calls only. Please see above for incidental personal calls.

C. Voice mail

1. Each employee may receive voicemail service for their telephone extension. Employees should check voicemail regularly, and then remove old messages from the system.

VII. Software Usage and Standards

A. Peer-to-Peer software

1. The use of any Peer-2-Peer (P2P) file-sharing application to download copyrighted material is prohibited. These types of software cause network congestions as well as installing "Spy-ware" on a users PC.
2. List of commonly used P2P file sharing applications that are prohibited (not all inclusive): KaZaa, WinMX, Morpheus, Bearshare, XoloX, iMesh, Blubster, Grokster, and Limewire.
3. Please note that this type of software will be removed from computers when found.

B. Ad and Spy Software

1. Users should take extreme caution when browsing the Internet as well as installing "unknown" software. Many websites ask you to install their search toolbar or other "browser enhancement" software. These types of software applications should not be installed due to the probability of being embedded with "spyware" or "adware". Please note that this type of software will be removed from computers when found. The Google Toolbar is an exception and may be used.

C. Virus Protection Software

1. All computers on campus must have virus protection software installed. If technically possible, computers that do not have virus protection software will not be allowed on the LSUA network. Each computer that is configured by IET Services will automatically have virus protection software. This software will be configured to update on a daily basis.

VIII. Data Storage, Backup and Recovery

A. Network Storage Space

1. Each user with an Active Directory account will be given access to a network-based storage space for storing personal files. This is referred to as the "Y:" drive for employees and "X:" drive for students.
2. Each department will be assigned a network storage space for sharing files within the department. This is referred to as the "W:" drive.
3. Any information stored on either of these drives is backed up according to the schedule set forth in this document. Users should store data on network drives whenever possible. This is the only way to ensure against data-loss if the local computer hard drive is corrupted.

B. Data Backup

1. Schedule of backups for Network Data
   All data stored on network based devices will be backed up according to a regular schedule. This schedule may change on a periodic basis, and therefore is not a part of this document. A complete backup schedule of network-based data is available in IET Services.
2. Backup of Users Data on local Computers
   Each user is responsible for making backup copies of critical data that is stored on their assigned computer. Data stored on computers around campus cannot be backed up across the network on any defined schedule. Network storage space such as Y: and W: drives should be used whenever possible for the storage of critical data and documents.

C. Data Recovery

Data stored on network-based devices maybe restored at anytime by request from the owner of that data. Data will be restored from the latest available backup according to the current backup schedule.

IX. Web Usage and Standards

Louisiana State University at Alexandria is committed to providing timely and accurate information to its prospective students, current students, alumni and friends, faculty and staff. The University recognizes the use of the Internet and the World-Wide Web as avenues for communicating with all its constituencies.

A. Webmaster Responsibilities

1. The University Webmaster shall be defined as the Coordinator of Web Services or his/her designee. The person shall be the point of contact for all administrative, departmental, divisional, and organizational web-related services.
2. The Webmaster can route requests and inquiries to the appropriate personnel charged with addressing the issue raised, e.g. questions of policy would be forwarded to the ITAC; requests to link new/redesigned sites to LSUA's top-level pages would be routed to the ITAC web subcommittee; project work would be performed by the Webmaster, her/his staff and/or other staff as needed.
3. The Webmaster is responsible for all campus web services provided by multiple persons and departments. Specific charges are to:
    a. Serve as point-of-contact for available campus web services
    b. Provide administrative web programming and support
    c. Maintain the IET Services web site along with those determined by the ITAC web subcommittee.
    d. Review and provide data regarding LSUA's web presence and utilization.
    e. Recommend and promote adherence to appropriate policy
    f. Provide training and/or consultation to department/organization webmasters.
    g. Work in conjunction with IET Services employees to maintain network servers and related equipment associated with web services.
    h. Monitor web site statistics and recommend changes and upgrades when necessary.

B. Governing Committees
   1. ITAC
      a. The ITAC is a University group responsible for establishing and monitoring University-wide technology initiatives, standards, priorities, and policies. The group also works with IET Services to review progress on technology initiatives, to provide feedback, and to serve as a forum for communication. The ITAC is chaired by the Director of IET Services.
      b. The purpose of ITAC in regard to the web is to:
         (1) Review and act upon changes or issues regarding the top-level pages or other public relations-related issues brought to the committee, and
         (2) Approve the linkage of new or updated sites to the appropriate top-level page
         (3) Review the University image and information published on all official, non-personal University web sites.
   2. Campus Webmasters Users Group
      a. This group exists to facilitate communication of policies, procedures, information, and training to the campus webmasters who are individually responsible for the content management and timeliness of all official, non-personal campus websites.
      b. This group will also serve as a forum for intra-communication among the webmasters. The University Webmaster, along with other staff as needed, will be providing technical assistance and support for all campus webmasters. The Webmaster will also chair the committee. Area supervisors should initially identify area webmasters. Although, the Webmaster can provide start-up service, special project, and technical support, it shall be the responsibility of each official, non-personal University "area" to provide content and maintenance for their own web site unless otherwise agreed upon by the ITAC web subcommittee.
      c. This group should meet at least once per month for updates and training.

C. Publishing Information via the LSUA Web Server
   1. Those who publish web pages at the University shall comply with the following policies and ethics:
      a. Developers must adhere to the policies outlined within this document.
      b. The University web servers shall not be used for commercial, profit-seeking purposes, or to advertise goods and services unless officially sponsored by the University as set forth by LANET and the Office of Telecommunication Management (OTM).

2. Departmental/Area Web Pages
   a. Departments are responsible for the development of their own web pages. This approach allows the department to control the timeliness and accuracy of its information. All aspects of page development, including compliance with University policies and timely updating of all page elements, are ultimately the responsibility of the department heads. It is the responsibility of the department to follow acceptable-use and other applicable University policies.
   b. When a department's Webmaster responsibilities shift to another individual, the University Webmaster must be informed of the new area Webmaster's name and e-mail address. E-mail notification may be sent to webmaster@lsua.edu.
   c. Departmental webmasters are highly encouraged to use official banner graphics and navigation bars available from the Webmaster to identify at least their homepage. Every page on official web sites must minimally include:
      (1) A clearly visible link to the University home page (may be included in copyright statement in the page footer)
      (2) A link to the University webmaster (address must be visible on the page)
      (3) A link to the departmental/subject matter webmaster (address must be visible on page)
      (4) Date of last page modification – If sites are updated at least every six months. Departments who cannot or are not updating at least this frequently should remove "last updated" references from their pages.
   d. The Webmaster will provide templates that match the University "Top-Level" sites to area webmasters on an as-needed basis.
   e. After new site creation or major updates to existing sites, the ITAC web subcommittee must clear approval for linkage from LSUA top-level pages. Requests should be routed through the Webmaster.
3. Organizational Web Pages
   a. Organizations officially recognized by the University may publish web pages on the University's web server. The sponsor and a single organizational contact person must be identified via appropriate forms filed with IET Services. This request form is available at http://iet.lsua.edu/webservices/. All aspects of web page development, including compliance with University policies,

are the responsibility of the sponsor and members of the organization.

b. Every page must include a clearly visible link to the University home page, (may be included in copyright statement) the organization Webmaster's current e-mail address (visible on the page), and the date of last page modification. Links to organizational web pages from LSUA's top-level pages are subject to ITAC web subcommittee approval.

4. Faculty, Staff, and Student Web Pages

a. LSUA allows server space on a separate server/s for personal web pages as a service to the University community. Personal pages are not part of the University's official web pages. Each web creator bears sole responsibility for the content and maintenance of his or her personal web files.

b. The University does not endorse the contents of these pages nor can it accept any responsibility for the information contained therein.

(1) That said, the use of LSUA web space is a privilege. Individuals who use the University's computing resources are obligated to adhere to all University policies, including those identified within this document.

D. General Web Policies

1. Ownership of Data

a. The University owns the top-level web pages, departmental web pages, and web pages (other than course work and faculty research materials) residing on any web server owned by the University.

b. The University reserves the right to manage any University-owned computer resource as it sees fit. The University reserves the right to identify materials on University-owned resources that violate copyright.

2. Additional Design Considerations

a. Due to standards of professional web design and University identity, images and text endorsing a particular web browser (such as "Best if viewed with Netscape Navigator 4.5") are discouraged. University web developers must design their pages for the largest portion of visitors possible.

b. Wherever possible, links to off-site locations should be coded in such a way to cause the link to open in a new window or be clearly noted, making it clear to visitors that they are leaving the LSUA domain.

3. Publicity and Advertising on Official University Pages

Publicizing non-University-affiliated events, opportunities, and products on the University's website may be done when such publicity is:

a. Within the scope of the mission of a particular campus department or organization.

b. Done with the permission of the department head/director/sponsor of a particular department or organization.

c. Contained within the web pages associated with the appropriate department or organization.

4. Assistance

a. A web site with resources, tutorials, tips, and off-site links shall be maintained to support University webmasters at http://iet.lsua.edu/webservices/.

b. Periodic training sessions will also be held campus webmasters or other appropriate personnel.

E. Web Site Nomenclature

1. Introduction

a. LSUA maintains multiple web servers, multiple web sites, which are "official" (yet, subordinate to the University top-level web site) and multiple personal web sites. In order to facilitate some standardization of nomenclature the following policies will apply:

2. Policy

a. The University's home page and top-level navigational pages shall be found at: **http://www.lsua.edu**

b. Information which is not explicitly the content for existing departments or offices will be subordinate to the home page in the following manner:

http://www.lsua.edu/file-name.ext

or

http://www.lsua.edu/folder-name

c. All colleges, academic disciplines, departments, chartered organizations, and other official administrative web sites shall follow the following naming structure:

http://department-name.lsua.edu

d. Sub-departments, programs, and department intranets should be subordinate to the main organization's URL as follows:

http://department-name.lsua.edu/program-name

e. Individual faculty, staff, and students may not have accounts (other than for technical/testing purposes) on the administrative web server. Accounts on the personal servers will follow the structure of:

Faculty: http://facultypages.lsua.edu/username
Staff: http://staffpages.lsua.edu/username
Students: http://studentpages.lsua.edu/username

3. Naming Conventions

a. There are a number of internal guidelines and Internet RFCs that dictate the syntax of a domain name.

b. In summary names must be:

(1) Recognizable as the organizational unit for which the website is named
(1) 63 characters or fewer
(3) ASCII letters, digits and the hyphen character
(4) Cannot be all digits, but can begin and/or end with a digit.

X. DEFINITIONS

A. LSUA – Louisiana State University Alexandria

B. Technical Resources – any computing resource, including but not limited to, IBM compatible computers and associated peripherals, networking equipment and infrastructure, mainframe systems, servers, telephone systems and/or any other electronic or computing based system, service, or equipment owned or operated under the supervision of LSUA.

C. University Network – The University network is defined to include any and all computer and electronic based communication facilities and/or equipment, which are owned or operated under the supervision of LSUA. The University network is for use by authorized personnel affiliated with the University, consistent with, and in the course of, their official work, study, and/or research.

D. User Account – A User Account is an account assigned to a specific user of LSUA technical resources. The following are types of User Accounts available at LSUA: Active Directory, Mainframe, Administrative Software, Local Computer, Course Management System (CMS), myLSUA, Pass-Port, and/or any other technical resource that requires a user to be “logged-on”.