LSU SHREVEPORT

POLICY STATEMENT: No. 1 17.04

COORDINATED BY: Division of Business Affairs / Office of Information Technology Services

EFFECTIVE: April 4, 2011

SUBJECT: COMPUTER ACCESS AND USAGE

1.0 Purpose

Louisiana State University in Shreveport (LSUS or University) hereby establishes this information technology and data security policy that creates a framework for the use of data, applications, networks and computer systems. This Computer Access and Usage Policy provide guidelines for users of the LSUS information system. The scope of this policy includes the systems themselves, the hardware that these systems run on, and the personnel that use and support these systems. The policy statement is designed to fulfill PM-36 and Office of Information Technology (OIT) policies/standards. The appropriate portion of PM-36 and OIT policy/standard will be denoted in brackets. [PM-36 1.1.1]

2.0 Jurisdiction

The LSUS Office of Information Technology Services (hereinafter “ITS”) is charged with:

- Maintaining the Network
- Maintaining Network Security
- Growing the Network
- Approving Computer Purchases
- Approving Computer Specifications
- Approving All Network Additions/Modifications
- Managing All Enterprise Wide Software Patches and Antivirus Software

All functions providing a campus wide computing resource of any kind will be run by ITS (i.e., registration service, calendaring services, web pages, etc) and housed within the protected server room located in the Administration Building.

Individual academic departments may create labs for their department specific students. However, ITS reserves the right to require these labs to be adequately protected with up-to-date patches and virus scanning software. These labs will be placed behind a firewall in order to provide network security. Personnel in those departments which are behind firewalls who need to access administrative resources will be required to use VPN clients or alternate secure access methods. No security hole will be created in the network to support inter-departmental communication or lab communication.

3.0 Ownership & Possession

All computers, computer peripherals, and software purchased with state money, institution money, grant money, or donated to LSUS are the sole property of LSU in Shreveport.

All software/hardware created on state time and/or with state equipment falls under the rules of PM-16.

4.0 Types of Information

The importance of the information used in the course of business at any business can not be underestimated. LSUS has a variety of types of information that flows through our networks and computer systems daily. Some of this information may be trivial, but most information must be protected and secured.

LSUS maintains a database of information assets which includes rankings of each information asset with regard to confidentiality, integrity, availability, and criticality to operations. [PM-36 12.1.1]

LSUS has adopted a method to classify its electronic protected or restricted information according to the level of confidentiality, sensitivity, value, and criticality. This method is not less restrictive than the method defined by Louisiana state law and/or the State of Louisiana Office of Information Technology. [PM-36 12.1.2] The classification system incorporates four levels. In increasing order of restrictions, the levels are public, internal, protected, and restricted. Public information can be defined as information with no restrictions and can be released to the general public in accordance with university policy. Internal information can be defined as information regarding the internal business and education operations of LSUS. Examples of internal information include but are not limited to emails, memos, management and operational reports. Internal information may not be disclosed without approval of the management of the appropriate department of the LSUS campus.

Protected information is information that shall have extraordinary controls over its use and disclosure due to the sensitivity of its content. Examples of protected information include, but are not limited to: employment records, medical records, student records, personal financial records (or other individually identifiable information), research data, trade secret information and classified government information. Protected information shall not be transmitted outside the confines of the LSUS campus network without the use of appropriate safeguards to preserve its confidentiality and integrity. Protected information shall not be shared with contractors or other business associates without an approved agreement in place governing the use, handling, and disclosure of the confidential information. Any unauthorized use and/or disclosure of protected information shall be reported to the Chief Information Officer immediately. Should it become necessary to disclose protected information in order to provide requested services to an individual or comply with existing laws and regulations, the information disclosed shall be the minimum necessary to perform the service or comply with the legal requirement. [PM-36 12.1.3]

Restricted information is information of such a sensitive nature that access is limited to those individuals designated by management as having a need to know. Examples of restricted information include, but are not limited to that related to ongoing investigations, pending litigation, psychological notes and disciplinary action. LSUS shall take appropriate measures to ensure that restricted information is not disclosed to anyone other than to those individuals designated by management. [PM-36 12.1.4]

This document is public information and is available for any interested individual.

5.0 Grant of Security

Information is an LSUS and state asset that must be protected from unauthorized access, use, modification and destruction. Upon employment or enrollment at LSUS, users are given a grant of security which will allow them to use computers and information at LSUS. The access given to them is appropriate with their role in the institution and may be modified or restricted as best for the University.

Their access is based upon an ITS user-ID and password which is provided to them.

Access to data or resources in any computer system with the most basic level of security most often requires the user to identify him and prove his identity. The user's identification (user-ID) tells the system who the user is and the user's password proves, or authenticates, the user's identity. Once the system knows who the user is, it can determine what data and resources the user can access.

Access to any LSUS campus information system shall be authorized by the owner and/or campus designated official(s). Each faculty, staff, student, and contractor shall be assigned a unique user ID. ITS will provide a department with a generic id when it is required by operational necessity. For audit purposes, such access, including the appropriate access rights or privileges, and a record of the authorization shall be maintained by the user's department for six years after the access is terminated. [PM-36 2.1.2, 2.1.11]

The authentication process provides protection by controlling access to the assets of information technology systems. Authentication techniques permit validation of user's identities, hardware devices, and/or transmitted information.

Student user-IDs and passwords are generated after the registration period has ended for the semester. The student's become aware of their IDs and passwords based upon a common creation schema which is both posted on the LSUS website and provided to them through their professors. Their ID and password allows them access to the student email system, the myLSUS registration system, the Moodle learning management system, and the LSUS wireless network.

Faculty and staff user-IDs and passwords are generated for a staff member when it is requested of the Chief Information Officer by their supervisor. Because of the variety of tasks they may be asked to participate in, their access is individualized.

If the user needs student record access, class scheduling access, chair access, or dean access, supervisors should be prepared to note this in their request to the Chief Information Officer.
If the user needs budgetary access, supervisors must send a request to the Director of Accounting Services requesting this access be provided.

If the user needs payroll approval or entry access, supervisors must send a request to the Director of Human Resources requesting this access be provided.

Their ID and password allows them access to the faculty/staff email system, the myLSUS registration system, the LSUS Unix system, the Moodle learning management system, the LSUS wired network and the LSUS wireless network.

In response to an emergency (*i.e.*, an employee is incapacitated and another employee must enter the system to continue his job function), the Vice Chancellor of the proper division should provide a written request to ITS indicating what employee should take control of the job function during the duration of the emergency. Each instance of such access provision shall be documented and shall be maintained on file in employee's department for a period of no less than six years, if the information accessed is protected information. [PM-36 2.1.11]

Please note that those employees taking personal days, attending conferences, or otherwise gone in a planned manner, should make arrangements prior to their leave, such as delegating budget access, etc. These situations and temporary illnesses are not cause for the provision of emergency access. This clause is meant to deal specifically with unusual and unexpected situations.

5.2 Transmission and Encryption

Restricted or protected information shall only be transferred outside of LSUS networks, or copied to other media, when the confidentiality and integrity of the data can reasonably be assured. [PM-36 3.4.1]

One way that the confidentiality and integrity of the data can be assured is via secure encryption technologies.

Encryption is the translation of data into a secret code (cipher text) that is only readable by the intended recipient. To read or decrypt an encrypted file, the recipient must have access to a secret key, certificate, or password. Decryption is the conversion of cipher text into plain text.

Office of Information Technology Standard 23 identifies the minimum acceptable technical features of encryption for use by state agencies.

5.2.1 Via Fax Machine/Fax Modems

Protected or restricted information shall only be faxed when more secure methods are not available. [PM-36 1.2.3] The sender of the protected or restricted information and the intended recipient should agree to the fax transmittal prior to sending.

5.2.2 Via Modems/ISDN/DSL Connections

Protected or restricted information shall only be sent via non-LSUS network lines when more secure methods are not feasible. In that event, additional precautions e.g. encryption of data, virtual private networks, etc., shall be employed to ensure against unauthorized interception and/or disclosure of protected information. [PM-36 1.2.4] The sender of the protected or restricted information via modem/ISDN/DSL connections and the intended recipient should agree to the transmission prior to sending.

5.2.3 Via Printer

Protected or restricted information shall not be sent to a network printer in an unsecured area without appropriate physical safeguards or an authorized person present to safeguard this information during and after printing. [PM-36 1.2.5]

5.2.4 Via Removable Media

All protected or restricted information stored on removable media, including diskettes, CDs, DVDs, flash drives, USB keys, and external hard drives, shall be kept in a safe, secure environment in accordance with the manufacturers' specifications when not in use.

The removal of protected or restricted information from campus premises shall require specific written authorization from the employee's direct superior. [PM-36 1.3.1]

5.3 Identity Information

Access to data or resources in a computer system with the most basic level of security requires the user to identify him and prove his identity. The user's identification (user-ID) tells the system who the user is and the user's password proves, or authenticates, the user's identity. Once the system knows who the user is, it can determine what data and resources the user can access. [OIT-Policy-006]

Information is a state asset that must be protected from unauthorized access, use, modification and destruction. The authentication process provides protection by controlling access to the assets of information technology systems. Authentication techniques permit validation of user's identities, hardware devices, and/or transmitted information. [OIT-Policy-006]

Authentication is the verification of the identity of a person or process. A password is a secret series of characters that, by association with a user-ID, allows access to information, systems, applications, or networks. [OIT-Standard-009]

All LSU information systems that use passwords as the primary method of user authentication shall require that all user accounts be password protected with non-null weak passwords and require all users to change passwords no longer than every 30 days. [PM-36 2.1.6] LSUS has developed a standard for password length, password change interval, and password complexity that are consistent with the State of Louisiana Office of Information Technology policy. Due to security concerns, these standards are not published in this policy. However, they are available to University personnel and contractors only as necessary upon written request to ITS.
LSUS campus faculty, staff, and students are expected to treat passwords as private and highly confidential. [PM-36 8.2.1] LSUS employees and other users of LSU computing resources must use reasonable efforts to protect their passwords.

Lending of keys, both physical and electronic is prohibited by LSUS. In the event that access to an area or information secured by a physical or electronic key is required by an individual without such key, that individual should be accompanied and supervised by someone who has been issued such a key.

LSUS shall ensure that the Chief Information Officer is notified of all employee terminations and that access to LSUS campus information systems is revoked. If in the judgment of the appropriate campus official, it is determined that an employee represents a risk to the security of LSUS campus information, all access shall be terminated immediately. Please see the LSUS Employee handbook for further information on this procedure. [PM-36 8.3.1, PM-36 8.3.2]

6.0 Grant of Usage [PM-36 2.1.9]

The computing facilities at LSUS are provided for the use of LSUS students, faculty and staff in support of the programs of the University. These users are required to show proper and ethical use of computers, software and related networks at LSUS. In providing access to knowledge and sharing of information, the University requires that these resources be used by all members of the university community with respect for the public's trust through which the resources have been provided.

LSUS computing resources are defined as all university owned computers, peripherals, networks, software and supplies.

Computing resources and accounts are owned by the University and are to be used for University-related or supported activities only. All access to departmental computing resources must be approved by the appropriate department chair or authorized representative. All access to central computing resources, including the issuing of passwords, must be approved through ITS.

All users of LSUS computing resources are held responsible for using the resources in an ethical and lawful manner. Access to LSUS computing resources is a privilege, and may be revoked if abused. Use of the resources for commercial purpose is prohibited.

An account assigned to an individual, by ITS or a department, must not be used by others without explicit permission from the individual requesting the account and by ITS or department assigning the account. The individual is responsible for the proper use of the account, including proper password protection.

LSUS reserves the right to monitor computer usage, accounts and files. Fraudulent, harassing or obscene messages or materials may not be sent or received electronically.

No one may deliberately attempt to impair the performance of the computer resources or to deprive authorized personnel access to University resources.

LSUS computing resources may not be used to obtain or copy computer software or data protected by copyright.

LSUS will take the following action against an individual who abuses or has gained unauthorized access to computer resources:

- The login id may be inactivated immediately.

- The appropriate administrative authorities and law enforcement authorities (LSUS, state or federal) will be informed.

- Actions taken by administrative authorities will depend on the severity of the computer abuse. The LSUS Code of Student Conduct, Louisiana House Bills 1801 and 430, Title 18 of U.S. Code 1030, Title 18 of U.S. Code 2701 as well as other state and federal laws will be used in determining appropriate action.

- Temporary actions may be taken to protect computing resources, persons, or property, while a determination is made whether any prohibited use or unauthorized access has occurred.

6.1 Acceptable Use

Internet access and email use facilitate LSUS in meeting its business needs. Internet access and email are considered LSUS property and LSUS has the right to monitor all use of such property at its discretion. With the exception of information protected by federal/state statutes and agency policies, users should have no expectation of privacy as to their Internet and email usage via LSUS computers and networks. [PM-36 2.1.5]

The purpose of Internet and email use via LSUS resources is to conduct official LSUS business. LSUS may determine availability of Internet and e-mail services on LSUS resources based on employee need and use.

Acceptable use must be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanisms, and individual rights to privacy and freedom from intimidation, harassment and annoyance. Users are held accountable for any breaches of policy, security, or confidentiality resulting from their use of the Internet or email. An abuse of the privilege of Internet or email use on LSUS resources may result in disciplinary action as deemed appropriate by the supervising authorities up to and including termination of employment. Use of the Internet and email as described below is acceptable:

- To provide and facilitate official state business (intra-agency, state and federal agencies and business partners of state agencies).
- To use for professional society, university association, government advisory, or standards activities related to the user’s employment-related professional/vocational discipline.
- For informational purposes or to discuss political issues related to LSUS. However, the following statement must be contained in any such usage: *The views expressed are my personal opinion and do not represent the views of LSUS nor that of the LSU System.*
- Other uses not in violation of this policy that may be allowed or required by individual department or agency policy.

6.2 Prohibited Use

Appropriate *University administrative offices* may establish and maintain procedures necessary to investigate, receive, and resolve allegations of abuse, misuse, or prohibited use of LSUS *computing resources*.

Specifically each *user* of LSUS *computing resources* shall **NOT***:*

- Download, store, transmit, or display any kind of image or document using any department system or resource that violates federal, state, or local laws and regulations, executive orders, or that violates any LSU System, LSUS, or department-adopted policies, procedures, standards, or guidelines.
- Obtain or use another's logon ID or password, or otherwise access *computing resources* to which authorization has not been expressly and validly given.
- Use another's log-on identification or password to hide their identity or attribute their use of *computing resources* to another.
- Copy, install, or use any software data, files, or other technology that violates a copyright or license agreement. In particular, each *user* should not distribute or download copies of copyrighted material for entertainment or personal use without explicit permission from the copyright owner.

  NOTE: *Copyright law applies to materials such as games, movies, music or software in both analog and digital format.* ***User(s) shall not download an illegally distributed file to a computing resource.*** *Copyright holders regularly notify LSUS of infringing activity using the procedures outlined in the Digital Millennium Copyright Act of 1998 (DMCA) and other legal procedures. As a service provider, LSUS must investigate complaints and take action to remove unlawful material. The law provides means for a copyright owner to obtain the identity of a subscriber.* ***If you illegally possess or share copyrighted materials, you may be denied access to LSUS's computing resources, be subject to disciplinary actions via the Office of the Dean of Students and/or Human Resource Management, and possibly face civil and/or criminal legal proceedings and sanctions. Please see:*** ***http://www.copyright.gov/legislation/dmca.pdf for more information***

- Utilize *computing resources* for political solicitation or to endorse political candidates.
- Utilize *computing resources* to create, transmit, or otherwise participate in any pranks, chain letters, false or deceptive information, misguided warnings, pyramid schemes, or any fraudulent or unlawful purposes.
- Utilize *computing resources*, including the Internet and/or e-mail to access, create, transmit, print, or download material that is defamatory, obscene, fraudulent, harassing (including uninvited amorous or sexual messages), threatening, incites violence, or contains slurs, epithets, or anything that may be reasonably construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, age, disability, or religion or to access, send, receive, or solicit sexually

oriented messages or images or any other communication prohibited by law or other University directive.

- Intentionally or knowingly copy, download, install, or distribute a computer virus, worm, “Trojan Horse” program, or other destructive programs, or otherwise harm systems or engage in any activity that could reasonably and foreseeably disrupt services, damage files, cause loss of data, or make unauthorized modifications.
- Monopolize or disproportionately use shared *computing resources*, overload systems or networks with endless loops, interfere with others’ authorized use, degrade services, or otherwise waste computer time, connection time, disk space, or similar resources.
- Add, modify, reconfigure, or extend any component of the University network (*e.g.*, hubs, routers, switches, wireless access points, firewalls, etc.) without express, written authorization from the Chief Information Officer.
- Accept payments, discounts, free merchandise, or services in exchange for any services provided through use of the *computing resources*.
- Endanger the security of any *computing resources* or attempt to circumvent any established security measures, for any reason, such as using a computer program to attempt password decoding.
- Acquire, store, or transmit any hardware or software tools that are designed to evaluate or compromise the security of *computing resources* without the express written authorization of the Chief Information Officer.
- Send unsolicited mass mailings or “spamming.” Mass mailings should only be sent to clearly identified groups for official purposes, and may not be sent without proper authorization and coordination (for example, disseminating administrative announcements, notifying students of educational opportunities, or University organizations sending announcements to their members).
- Utilize *computing resources* to develop, perform, and/or perpetuate any unlawful act or to improperly disclose confidential information including, but not limited to, IP spoofing, packet capturing and/or port scanning.
- Taking any steps that block the University’s access to files and data, other than the use of University passwords, or approved encryption programs, unless such conduct is consistent with the University’s educational and academic policies or otherwise properly approved by the University.
- Install, store, or download software from the Internet or e-mail to University *computing resources* unless such is consistent with the University’s educational and academic policies or otherwise approved by the Chief Information Officer, in writing.
- Copy, impair, or remove any software located on any *computing resources* or install any software on any *computing resources* that impairs the function, operation, and/or efficiency of any *computing resources.*
- Utilize or access *computing resources* anonymously or with share-user identifications.
- Loading or using any program or software to hide, erase, disguise or overwrite any use of *computing resources*.
- Engage in any acts or omissions to intentionally or unreasonably endanger or damage any data or the security or integrity of any *computing resources.*

- Allow or assist others to utilize *computing resources* in a manner that is in violation of this Policy Statement.
- Access, add, or modify any data without proper authorization.
- Utilize *computing resources* in furtherance of or in association with any crime or violation of the Code of Student Conduct or other University policy or directive.
- Link non-University websites to or with University websites without the prior written authorization of the Chief Information Officer. Links to personal or private sector websites will only be approved to the extent they further the mission of the University.

Sanctions: <u>*Prohibited Use*</u> may result in sanctions, such as terminating access to *computing resources*, employment discipline up to and including termination of employment, civil liability, and/or criminal sanctions. The University may temporarily suspend or block access to any account or *computing resources*, prior to the initiation or completion of such procedures, when it is reasonable to do so in order to protect data or the integrity, security, and functionality of *computing resources*, or to otherwise protect the University or its students and employees.

Reporting: Security breaches and apparent or suspected *prohibited use* of LSUS *computing resources* should be immediately reported to the Chief Information Officer. Where violations of the policies and procedures governing *computing resources* and/or of law are alleged, appropriate law enforcement and/or *University Administrative Offices* may be contacted. Failure to report prohibited use is grounds for employment discipline and for terminating access to *computing resources*.

6.3 Portable Computing Devices (including Laptop/Portable Computers, PDAs, Cell phones, and other Portable Electronics)

Laptops and other portable computing devices issued to LSUS campus employees shall not be used for activities unrelated to LSUS organizational goals. The designated campus official shall document who is in possession of each device and that the individual understands his responsibility for the confidentiality, integrity, and availability of the information on said device. Each LSUS campus employee who is assigned a portable or mobile computing device shall be responsible for ensuring that data stored on that device is properly backed up, that the operating system is updated in a timely fashion, and where applicable, anti-virus software with current virus data files (including spyware detection and firewalls) is installed and running continuously. [PM-36 1.4.2]

6.4 Removal of Equipment or Data Offsite

Only authorized personnel shall be permitted to take any equipment belonging to LSUS off the premises and are responsible for its security at all times. [PM-36 1.4.2]

The removal of protected or restricted information from campus premises shall require specific written authorization from the employee’s direct superior. [PM-36 1.3.1]

7.0 Purchasing/Movement/Disposal/Sanitization/Damage

7.1 Purchasing

All proposed information systems to be purchase with LSUS funds (including donations, grants, etc.) shall be submitted to the Chief Information Officer for review for adherence to university hardware, software, and security standards, and approval prior to purchase. [PM-36 1.1.2]

7.2 Movement/Transfer

IT equipment and/or media owned by LSUS which is to be reassigned to another employee or reused shall be evaluated as to whether protected or restricted information needs to be purged in accordance with the National Industrial Security Program Operations Manual (DOD standard 5220.22M) and the Louisiana Office of Information Technology policy prior to reassignment and/or reuse. [PM-36 1.6.1] The moving or modifying of computer equipment, software or peripherals without proper authorization is prohibited. Moving or modifying of computer equipment or peripherals should be coordinated through Property Control in Business Affairs. Moving or modifying of software should be coordinated through ITS.

7.3 Disposal

IT equipment and/or media owned by LSUS shall only be disposed of by ITS and Property Control personnel in accordance with the National Industrial Security Program Operations Manual (DOD standard 5220.22M) and the Louisiana Office of Information Technology policy. [PM-36 1.6.1]

Disposal of information systems software shall not occur unless the disposal is authorized by the appropriate campus official, the information systems software is no longer required, and its related data can be archived and will not require restoration in the future. [PM-36 4.2.2]

7.4 Data Sanitization

Magnetic storage devices, optical storage media and non-volatile memory devices that are surplused, transferred to another government entity or subject to destruction, must use a method of data sanitization compliant with the following data sanitization matrix that was adapted from DoD specification 5220.22M if the data is determined by the owner to be protected or restricted.

Data Sanitization Matrix
Adapted from DoD Specification 5220.22M

Media Procedure(s)

Magnetic Tape

Type I* a, b, or l
Type II** b or l
Type III*** l

Magnetic Disk

Floppies (e.g., 3.5inch, zip disks, etc.) a, b, d, or l
Non-Removable Rigid Disk (e.g., hard drives) a, b, d, or l
Removable Rigid Disk a, b, d, or l

Optical Disk

Read Many, Write Many (e.g., CD-RW) l

Read Only l
Write Once, Read Many l
(e.g., CD-R,CD+R, DVD+R)

Memory

Dynamic Random Access Memory (DRAM) c, f, or l
Electronically Alterable PROM (EAPROM) i or l
Electronically Erasable PROM (EEPROM) g or l
Erasable Programmable ROM (EPROM) k, then c or l
Flash memory (FEPROM) c, h or l
(e.g., USB drives, xD Picture cards)
Programmable ROM (PROM) l
Magnetic Bubble Memory a, b, c, or l
Magnetic Core Memory a, b, e, or l
Magnetic Plated Wire c or l
Magnetic Resistive Memory l
Nonvolatile RAM (NOVRAM) c, f, or l
Read Only Memory (ROM) l
Static Random Access Memory (SRAM) c, f, or l

Sanitization Procedure Key

a. Degauss with a Type I degausser.
b. Degauss with a Type II degausser.
c. Overwrite all addressable locations with a single character.
d. Overwrite all addressable locations with a character, its complement, then a random character and verify.
e. Overwrite all addressable locations with a character, its complement, and then a random character.
f. Remove all power to include battery power.
g. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
h. Perform a full erase as per manufacturer’s data sheets.
i. Perform h. above, then c. above, three times.
j. Perform an ultraviolet erase according to manufacturer’s recommendation.
k. Perform j above, but increase time by a factor of three.
l. Destroy – disintegrate, incinerate, pulverize, shred, or melt.

This information was extracted in part from the US Department of Defense 5220.22-M Clearing and Sanitization Matrix.

*Type 1 magnetic tape includes all tapes with a coercivity factor (amount of electrical force required to reduce the recorded magnetic strength to zero) not exceeding 350
oersteds.

**Type 2 magnetic tape includes all tapes with a coercivity factor between 350 and 750
oersteds.

***Type 3 magnetic tape commonly referred to as high-energy tape (4 or 8mm tape are examples), includes all tapes with a coercivity factor between 750 and 1700.

7.5 Reporting

All deliberate damage to or theft of LSUS computer resources shall be reported to the Chief Information Officer and the Director of University Police as soon as it is discovered. The Director of University Police may notify appropriate local, state, or federal law enforcement when necessary. [PM-36 1.6.4]

8.0 Installation

All hardware installations shall be planned, and parties impacted by the installation shall be notified and given the opportunity to comment prior to the proposed installation date. All equipment, systems, software, upgrades, and patches shall be fully and comprehensively tested and authorized by management prior to being converted to a "live" environment. The extent of planning and testing shall be reasonable given the size and complexity of the installation to ensure successful implementation with a minimal disruption of operation. [PM-36 1.1.3]

ITS shall be informed of all installations and, with certain exceptions, will perform the installations.

9.0 Network Specific

All LSUS information system networks shall be designed and configured to deliver high availability, confidentiality, and integrity to meet business needs. All networking including wiring, wiring closets, network equipment, servers and other equipment shall be under the control of ITS. [PM-36 2.1.4, 3.1.1, 11.1.1]

9.1 Fiber

LSUS maintains fiber between all primary campus buildings. This fiber is to be used for approved LSUS network information flow.

9.2 Copper

LSUS maintains copper connections to almost every campus room to assist in user workstations and classroom use. In the situation where a copper connection is not available for a networking situation, the department can request a cable be run at their expense.

9.3 Switches

LSUS maintains enterprise quality networking switches to pass traffic throughout the campus. Additional ports are available in most buildings, but in the case of port shortage, new connection requests may require the department to assist in the funding of switch purchasing.

9.4 Firewall/IDS/Packet Shaping

LSUS shall utilize a firewall between the LSUS network and the outside world as the first level of security. LSUS shall ensure via Group Policy that each machine has an antivirus client installed. Furthermore, LSUS shall scan all incoming and outgoing email for viruses and SPAM. Via WSUS, patches shall be pushed to each user to ensure that the operating system and Internet browser are up to date to prevent malware from infecting them. [PM-36 3.3.1]

9.5 Router

The LSUS primary Cisco router is the authorized point of electronic data entry and exit from the university. It is maintained by ITS and currently provides 50mbs for Internet Access. Though it is reiterated in several other points, no other networks may be joined/bridged to the LSUS network via modem, wireless, or other means.

9.6 Wiring Closet Security

All cabling in LSUS campus networks shall be secured to prevent unauthorized interception or damage. [PM-36 1.2.6]

Physical access to server rooms and network infrastructure closets shall be protected using all reasonable and appropriate safeguards. Strong authentication and identification techniques shall be used when they are available and can be reasonably deployed. Access will be given only to personnel authorized by ITS. [PM-36 2.1.7]

9.7 Wireless Networking

A wireless LAN (WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. IEEE standard 802.11 specifies the technologies for wireless LANs. Implemented as an extension to a wired LAN, WLAN's are typically found anywhere a traditional network cannot be deployed for logistical reasons.

Wireless LAN's do not have the physical security normally associated with wired networks. Wireless access point signals often travel well beyond the facility in which they are located. Therefore, it is relatively easy to eavesdrop on wireless networks from a position outside an enterprise's physical perimeter. The lack of physical security, coupled with the often-used default configuration settings makes WLAN's extremely vulnerable to hacker attacks. Properly configured wireless access points and use of the 802.1X authentication framework provide a level of security that is more than adequate for all but the most sensitive networks. The addition of VPN technology and two-factor authentication further increases the level of security.

Wireless LAN authentication must be consistent with IEEE 802.1X standards.

Wireless LAN equipment must be configured to provide the following capabilities/functionality:

- 128-bit Dynamic WEP or TKIP w/MIC
- Disable SSID broadcast
- SSID must not contain information relative to agency location, mission or name
- Static IP addressing when users are known (note: environments that provide roaming access may use DHCP)
- MAC filtering when users are known (note: environments that provide roaming access are not required to use MAC filtering)
- WLAN equipment configured for infrastructure mode only

Guidelines/Technical Considerations:

- A site survey shall be conducted prior to deploying a wireless network.
- Firmware for access points shall remain current with the latest releases from the vendor.

- Agency premises shall be scanned frequently to detect unauthorized wireless networks (rogue access points).
- Access points shall be configured (power settings) and strategically placed such that the signal footprint will remain within the agency premise, while meeting the agency requirements.
- Wireless access should never be a defacto permanent replacement for locations where a traditional wired network would work best.

9.8 VLANs

ITS has designed the network with building specific VLANs in order to strengthen security by creating smaller fault domains. This is important to note for users as some equipment can not easily be moved from place to place without the reprogramming of the IP address information.

9.9 Protection of Ports

Non-ITS approved hubs, switches or wireless access points shall not be allowed on the LSUS network. Systems are in place at LSUS to ensure that only allowed devices are accessing LSUS networking resources.

10.0 Network Server Specific

10.1 Physical Location

Network servers and equipment shall be located in locations designated by ITS. The primary housing of Networking Servers shall be in the protected server room in the administration building which provides its own air conditioning system, drop floors, and UPS protection.

All LSUS campus information systems hardware and media that contain protected or restricted information are located in areas that are protected from physical intrusion, theft, fire, flood, excessive temperature/humidity or other hazards. [PM-36 10.1.1]

LSUS requires all unauthorized individuals to sign in to gain physical access to the protected server room in the administration building.

10.2 Domain Name Services

ITS maintains the LSUS.EDU namespace and assigns all LSUS domain names for the campus. Both internal and external DNS servers shall be maintained and kept up to date.

10.3 Dynamic Host Control Protocol Services

ITS is the only entity on campus which is allowed to run Dynamic Host Control Protocol (DHCP) services. Rogue DHCP services are often installed by accident when users attempt to install unauthorized equipment such as hubs, switches, and wireless access points into a network. When a rogue DHCP server is giving out invalid IP addresses campus services can be impacted. All rogue DHCP services shall be shut down.

10.4 LDAP

LDAP-enabled directory services provide a means to share directory information with all agencies via standards-based LDAP clients and directory–enabled applications.

In order to fulfill the growing need for centralized access to information and to support web-based applications and portals, LSUS has developed the means of centralizing employee records for application access authentication, e-mail address management, and access authorization to other LDAP server-based lists of information, and provide for standards-based, centralized management of employee records.

In addition, the directory service is:

- scalable
- programmable
- will support directory-enabled provisioning
- will integrate seamlessly with the other stated standards, including the network operating system, workstation operating system, and applications.

Approved Standards**:**

- X.500 standards for global directory construction and replication across multiple servers.
- LDAP version 3 compliant access services, the preferred standard for read/write access to directories.
- Kerberos version 5 and X.509 for authentication.

10.5 Patch Deployment

Keeping computers patched with the latest OS and software updates not only adds new features but also helps to close security holes that have been discovered in software. ITS shall manage all enterprise wide software patches.

Patches to resolve software bugs shall only be applied when verified and authorized by ITS.

LSUS is currently using Microsoft Windows Software Update Services (WSUS) to push patches for Windows OS and Office Suite products.

10.6 Network Time Services

In order to accurately document and mitigate information security incidents, all LSUS information system clocks are synchronized regularly to the extent possible. Both of the LSUS domain servers are running NTP and synching to http://tf.nist.gov/service/time-servers.html.

10.7 AntiSpam/Email Filters/Email Disclaimers

All email and/or any other form of digital communication generated by LSUS' information systems that contains protected or restricted information, including data attachments, shall only be permitted after confirmation that such action is consistent with the restriction specified by the security classification of the information being sent. In addition, the file shall be scanned for the possibility of a virus or other malicious code. This scan is done to prevent malicious code from being delivered or executed on LSUS information systems via email. In no case shall protected or restricted information be sent outside the LSUS information infrastructure without taking precautions to ensure the confidentiality and integrity of the information. [PM-36 3.3.2, PM-36 3.3.3]

10.8 Backup

All LSUS information systems that contain protected or restricted information shall be protected by adequate backup and system recovery procedures. These procedures ensure the integrity of the data files. [PM-36 3.4.2, 3.5.1] The procedures can be found in the LSUS Disaster Recovery Business Continuity Plan.

10.9 Uninterruptible Power Supplies

Power surges and power outages can cause havoc within networks and with the day-to-day operations of the university. Uninterruptible power supplies (UPS) allow equipment to continue to function in the event of power failure for a variable duration of time based upon the model of the UPS.

Please note that UPSs are only stop gap measures. Power outages of a long duration will require the systems the UPSs are supporting to be shut down. For power outages of longer durations, generators are the traditional method of support. LSUS will procure a generator to support its critical business applications should power outages of a long duration occur.

All information systems identified as critical to LSUS campus operations shall be protected by an uninterruptible power supply adequate to provide continuity of services and/or orderly shutdown to preserve data integrity. [PM-36 1.2.1]

10.10 High Availability

All systems which require a high degree of availability shall be ensured continuous operation during power outages and hardware faults. [PM-36 1.2.2]

10.11 Network Operating System

The LAN server operating/network operating system (NOS) is the master control software that monitors/administers/controls all internal operations for the network server. This includes communications with other networked servers and clients via network interface cards and modems, managing security, authentication, authorization, reading and writing memory and storage devices, transfer of information to attached printers (file and print sharing), accepting management commands from both keyboard and mouse input and support for communication protocols, including TCP/IP.

LSUS’ standard NOS for the enterprise:

- provides a multi-purpose operating platform for all the significant infrastructure and business functions of the network including: file and print sharing, authentication services, applications, e-mail, database, communications, and Internet (Web) serving.
- integrates seamlessly with the standard desktop operating system and a wide range of business applications.
- provides a fully-integrated directory that handles user authentication, resource access control and resource management.

- is robust enough to support a hierarchical file and security structure that mirrors the structure of the enterprise that it serves.
- runs industry-standard applications built using industry-accepted programming languages.
- provides a rich set of system management tools.
- has a large installed user base and local training opportunities.
- has widespread certified technical support options.
- supports a wide variety of industry-standard printers.

Approved Product: Microsoft Windows Server OS

10.12 Client Management

Client Management software provides for the support of user workstations through software distribution, imaging, hardware and software inventory, operating system installation and migration, and remote control capabilities.

ITS support staff is required to support client environments that are continually growing in both size and complexity. Client Management software enable ITS staff to automate many support processes such as software distribution, imaging, and operating system migrations. Remote control capabilities allow ITS staff to provide remote support to clients thus improving efficiency in the support process. Inventory and reporting functionality provide increased capability for ITS staff to audit and manage user environments thereby enabling improved software license utilization and compliance and policy enforcement.

The following functions by the software and vendor are supported:

- The client management product provides reporting capability. This reporting capability includes a body of standard application reports as well as the capability to produce custom reports and queries. Accessibility for this reporting functionality should be supported via a web browser.
- The client management product provides software distribution capability. This distribution capability provides functionality for complete installation of packaged or custom software applications, targeted client installation based on distribution lists or distribution policies, distribution scheduling, and privilege elevation for installation on clients with locked down desktops.
- The client management product provides client remote control capability. This remote control capability includes the ability to access a client desktop from a remote location by taking control of the client’s screen and keyboard, and remote execution of programs and process control. Functionality is provided to require permission from the client for remote access of the desktop.
- The client management product provides ‘self healing’ capability for distributed applications. This self-healing functionality provides for the restoration of missing components, repair of system registry, and resolution of version conflicts.
- The client management product provides integration to Active Directory. Integration with Active Directory provides for management of software distribution and reporting of inventories by units defined within the Active Directory system.

- The client management products is compatible with existing statewide IT standards published by the Office of Information Technology.

Approved Products: Microsoft Group Policy Objects in conjunction with Microsoft Group Policy Management Console and Desktop Standard PolicyMaker

10.13 Website Credentials and Security

Only acceptable ports shall be allowed through the firewall to the web servers. SSL certificates shall be in place to encrypt the electronic discussion between user and server. Only authorized personnel who demonstrate the qualifications established by ITS shall be allowed to make changes to the campus website and other LSUS websites. [PM-36 3.3.5] For more information on website publication policies, please refer to LSUS policy statement No. 1 18.00.

11.0 Desktop Specific

11.1 Supported Hardware

A minimum hardware configuration for Windows/Intel based desktop workstations is required to support desktop software standards.

This hardware configuration is intended to establish the recommended minimum configuration for Intel compatible desktop workstations. All Intel compatible desktop purchases should adhere to this minimum hardware configuration or equivalent.
PC replacement should be based upon a five year equipment life cycle for mainstream PCs.

Approved Standards:
Please see the ITS website for current standards.

Approved Products:
Please see the ITS website for current products.

11.2 Supported Printers

Printers come in many shapes, sizes, and feature rich types. LSUS has found that Hewlett Packard printers provide the best basis for a stable printing environment. Printers which are destined to be on the network are recommended to be Hewlett Packard printers with Jet Direct cards installed.

11.3 Supported OS

The desktop operating system (OS) is the basic control software necessary to run computers. The OS controls most internal operations on a desktop computer including basic I/O operations such as reading and writing to/from memory and storage devices such as hard disk drives, floppy drives and CD-ROM drives. It controls the video display, keyboard, mouse, infrared control devices, printers, scanners, and communication devices such as modems and network interface cards. The OS includes communication protocols including the TCP/IP protocol that makes it possible to access the Internet for e-mail, file access/transport, resource sharing and access to the World Wide Web (WWW). The OS also makes it possible to run desktop software that enable computers to be productive office tools.

Identification, acceptance, conversion and use of a standard desktop OS is necessary for many fiscal, functional and practical reasons. A single standard simplifies training, support, knowledge transfer, cross-agency communication and collaboration. It improves and facilitates statewide network expansion. The adoption of a single OS standard offers the opportunity to negotiate enterprise volume purchase discounts and dramatically decreases the overall cost of ownership including technical support costs, upgrade costs, training and administration costs, transition expenses, and maintenance costs related to service pack issues and bug fixes. Listed below are functional requirements that are driven by business needs:

- Advanced security features and user control
- Administrator-assigned user levels that enable varying degrees of user rights
- Varying levels of password security that include system enforced password creation and scheduling rules
- Support multiple desktop profiles that can be managed by an administrator to create a common look and feel across the enterprise
- Seamless integration with functional and product desktop software standards
- A 32-bit OS with graphical user interface for Intel compatible platforms that supports the TCP/IP network protocol with multiple network services including remote access service.

Access to operating the system supervisor and/or administrator accounts should be restricted to those persons who are authorized to perform systems administration/management functions.

Approved Product: Microsoft Windows Desktop OS

11.4 Supported Office Suite

A collection of software programs sold together as an integrated toolset used on office personal computers to perform typical business functions, such as word processing, client email, numeric analyses, and presentation graphics.

Use of a common, integrated set of office programs to provide the workforce with:

- the ability to easily share memos, documents, numeric analyses, email messages, databases, graphic presentations, etc., within a department and between departments, without the need to convert files from one format to another, which can result in lost data, time, and productivity.
- a common scripting tool can be used to write macros that cross applications
- basic web interface and an integrated set of internet authoring tools.
- reduced training time and expense. Once an employee has learned how to negotiate word processing, they can more easily learn spreadsheets and graphics.
- Employees can leverage skills between products as they move within a department and between departments.
- simplified license tracking and seat management

Approved Product: Microsoft Office Suite

11.5 Supported Email Client

A robust electronic messaging system is comprised of intelligent e-mail (both "person to person" and "application to application") and task management, integrated with calendaring and group scheduling; contact management; web accessibility; flexible replication options for working off-line; and seamless integration with standard office software and a variety of wireless devices.

Electronic messaging is one of the most mission critical components of LSUS communication. It shall be robust, secure, and capable of growing as the enterprise grows. To simplify and enhance communication and collaboration, and encourage the sharing of information, a strategic asset of the state, a single electronic messaging system shall be used throughout LSUS.

Approved Product: Microsoft Exchange

11.6 Supported Anti-SPAM

Anti-SPAM is the technology (hardware and/or software) used to eliminate large percentages of unsolicited email, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.

SPAM costs LSUS monies not only in lost employee productivity (time to review/delete unwanted e-mail), but direct computer and bandwidth costs. These include increased need for storage, bandwidth, CPUs, wear and tear, etc. Direct non-computer costs include server room space, cooling, electricity -- and the personnel to handle both the increased traffic and the inevitable complaints from users.

Essential features and requirements include:

- Low Administration - easy to use tools and/or instructions
- Low False Positives - the capability to keep the false positive rate at or below .5%
- Email System Independent - must have the ability to operate independently of an organization’s existing mail system (Exchange, Lotus Notes, and GroupWise).
- SPAM Detection updates - consistent updates used to detect, filter, and/or reject spam.

Approved Products: Symantec Corporate Anti Virus and Trend ScanMail

11.7 Supported Anti-Virus

Anti-virus (or virus screening) software inspects computer system storage devices and media for any known or potential malicious code (viruses, Trojans, worms, hoaxes) hereafter referred to as a virus. A virus is a program usually disguised as something else that causes some unexpected and undesirable event, such as creating simple nuisance messages, to deletion of data on a hard drive, to overwriting the boot sector and making the computer system unusable. The growing use of the Internet has provided a mechanism for the fast and wide distribution of viruses and has led to a corresponding growth in the number and technical complexity of computer viruses. The purpose of this policy is to help protect all computing devices from malicious software. Industry best practices indicate the use of virus screening software, with regular updates and scan intervals significantly reduces the risk of virus contamination.

Enterprise wide antivirus software will be managed by ITS.

All firewalls, servers, personal computers and laptops shall have LSUS approved Anti-virus software.

Anti-virus software updates are applied when made available by the vendor.

Scheduled system scans for desktops occur daily during the work week.

Scheduled system scans for servers are determined by the agency, based on its' respective environment.

Non-state-owned computing devices (home user and contractor PC's) attached to the LSUS internal network must utilize anti-virus software with the current updates.

Approved Product: Symantec Corporate Antivirus

11.8 Supported Internet Browser and Viewers

A browser is a client program that uses HTTP to locate, display, and navigate between hypertext documents on the World Wide Web.
A viewer is a client program that allows a user to view "published" documents, regardless of the application or platform on which it was created.
Plug-ins extend the range of Web content available to a browser. Plug-ins make it possible to enjoy audio, video, and Web content in proprietary file formats.

Due to the variety of products used to publish documents that are served via the web, the selected browser must support a reader utility that will allow the user to view and use these files without having access to the original software used to create it, while preserving the original high-quality published look-and-feel.

Approved Products:

- Microsoft Internet Explorer
- Adobe Acrobat Reader
- Macromedia Shockwave
- Macromedia Flash
- Microsoft Media Player
- Real Networks RealPlayer

11.9 Power Management

A reduction in desktop energy consumption can occur by user intervention and the utilization of power management features within the operating system.

Users must logoff and power down desktop personal computers (system units, monitors, direct attached printers, scanners, external drives, speakers and other peripheral equipment) at the end of the work week (usually each Friday).

Users desktop PCs shall be configured by ITS to utilize the power management features of the operating system that place the monitor and hard disk drive in a “sleep” mode after a period of inactivity no greater than sixty (60) minutes.

Desktop PCs using applications that are not compatible with the operating system power management feature will be exempt from this policy.

11.10 Unattended Workstations and Logon/Logoff Procedures

Logon procedures shall be strictly followed. All computers will be required to run password and screen saver software in order to prevent unauthorized use. [PM-36 1.6.3, 2.1.3]

11.11 Pushing of Security Polices/Disclaimers

Upon access to LSUS domain computers on campus, users shall be presented before log in with a reminder that use of the computing systems at LSUS must adhere to this policy.

11.12 Pushing of Patches

LSUS has implemented procedures to adequately configure and safeguard its information system hardware, operation and application software, networks and communication systems against both physical attack and unauthorized network intrusion. All servers and work stations shall run anti-virus software (including spyware detection and firewalls) while connected to LSUS network infrastructure. In the event that the system will not operate properly with the anti-virus software, appropriate information security safeguards shall be instituted. [PM-36 3.1.3] All anti-virus data files shall be updated no less frequently than monthly. All adequately tested operating system patches shall be applied in a timely fashion.

11.13 Global Drives/Provisioning and Usage

ITS has provided global drives that are available to each department. Also provided are a drive that services each division and one which services the entire campus. These drives are to facilitate data sharing amongst users. This is the preferred method over doing Peer-to-Peer sharing.

11.14 Adhering to Licensing Agreements and Copyright for installed items

LSUS shall make every effort to ensure that all terms and conditions of End User License Agreements (EULA) are strictly adhered to in order to comply with applicable laws and to ensure ongoing vendor support. [PM-36 4.1.1]

Users should understand that while LSUS owns site licenses to many software packages, that the use of others (specifically Adobe Acrobat and SAS) is provided only to those departments/users who purchase the product.

Copies of software provided to users for home use under various licensing agreements is intended for ONLY their computer and ONLY for the duration of their employment with LSUS. Any other use is strictly prohibited.

11.15 Remote Access Software

LSUS users who utilize remote access via desktop PC's and laptops must ensure these devices are configured as indicated below. [PM-36 2.1.10]

Remote Access Requirements

	Access via Public Internet (ISP) (DSL, cable, dial-up, wireless)	**Direct Dial-In** **(RAS, etc.)**	**Dedicated Circuit** (point-to-point)
Employee (home)	AV software w/ latest signatures, Personal FW, VPN, Spyware removal software/service with latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, dial-back or 2-factor authentication, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only
Employee (on the road w/agency laptop)	AV software w/ latest signatures, Personal FW, VPN, Spyware removal software/service w/ latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, 2-factor authentication, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	
Contractor	AV software w/ latest signatures, Personal FW, VPN, Spyware removal software/service w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, dial-back, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only

Note:
VPN client software will be provided by LSUS ITS to those authorized to VPN into the campus.

Antivirus (AV) and personal *firewall* (FW) software on non-LSUS-owned input devices is the responsibility of the user. However, this software is not vendor-specific, but must be a current product with the latest updates/virus signatures.

11.16 User Restrictions – Modems

Modem hardware attached to or installed in desktop computer systems connected to the network is prohibited. Additionally, laptop users are prohibited from using simultaneous connections via the modem and the network interface.

12.0 Business Applications [PM-36 2.1.5, 2.1.9, 3.2.2, 3.2.4]

Only authorized staff may access operational program libraries. [PM-36 5.1.1]

Only authorized staff may access program source libraries. [PM-36 5.1.2]

All changes to systems, source code and operational program libraries shall be properly authorized and tested before moving to the live environment. [PM-36 5.1.3] Emergency amendments to software are discouraged, except in cases in which management has designated a circumstance as “critical”. Any amendments should strictly follow agreed upon change control procedures.

All software developed for systems identified as critical to campus operations shall always follow a formal managed development process appropriate for the size and scope of the system. [PM-36 5.2.1] All proposed new software development or system enhancements should be business driven and supported by an approved business case. Ownership (Responsibility for) such development or enhancements is assigned to the business owner of the system.

Only on rare occasions and with the approval of the Chief Information Officer shall ITS programming staff be allowed access to the production environment.

LSUS shall maintain a test environment for all systems identified as critical to campus operations. [PM-36 5.3.1]

All new systems shall be tested for capacity, peak loading, and stress testing. The new system will demonstrate a level of performance and resilience which meets or exceed the technical and business needs and requirements of the campus.

Normal system testing procedures for LSUS will incorporate a period of parallel running, when deemed necessary, prior to the new or amended system being acceptable for use in the live environment.

New and enhanced systems shall be fully supported by comprehensive and recent documentation. New or upgraded systems shall not be introduced into the live environment unless supporting documentation is available.

LSUS shall ensure that all vendor developed software meets the User Requirements Specifications and offers appropriate product support.

Users and technical staff shall be trained in the functionality and operations of all new systems. [PM-36 5.3.2]
Because our application system contains protected and restricted information, any attempts of unauthorized access and system errors shall be logged. These logs shall be examined by ITS staff to determine the extent and ramifications of the possible breach and followed up on appropriately. In addition, our application system also logs many authorized access transactions in order to provide a history of tracking changes. Some examples of this include a full record of all student registration transactions and a full record of all financial transactions. [PM 36 2.1.8]

If possible, transaction and processing reports shall be reviewed regularly to detect processing errors, system failure, human errors, natural disasters, and deliberate acts that may affect the integrity of electronic protected information.

13.0 Technical Support

All personnel responsible for managing the campus' network and preserving its integrity will report to and be managed by ITS. At the discretion of ITS personnel may be assigned to departments for day-to-day support. All personnel must meet ITS standards. [PM-36 3.1.2]

System administrators will be from ITS and they will mange the information technology systems; and oversee the day to day security of these systems. [PM-36 3.2.1]

Only qualified staff or third party technicians shall repair information system hardware faults.

13.1 Supporting of Applications

All LSUS application software shall be supported to ensure that the campus' business is not compromised. Every effort shall be made to resolve software problems efficiently and within an acceptable time period. [PM-36 4.2.1]

Equipment owned, leased or licensed to the LSUS campus shall be supported by appropriate maintenance facilities and/or qualified engineers.

13.2 Maintaining and Using of Documentation

Up-to-date system documentation shall be readily available to staff both online and via the web. [PM-36 1.5.1]

14.0 Off-campus Workers

LSUS allows teleworking (or working from home) provided the worker is ensuring the confidentiality, integrity and availability of the protected data accessed during any teleworking session. [PM-36 1.4.3]

15.0 Outside Contractors

Individuals responsible for commissioning outsourced computer processing of protected or restricted information shall ensure the services used are from companies that operate in accordance with the campus' information security standards with include a Business Associate Agreement or similar document that communicates the expectation of compliance with these standards and the remedies available in the instance of non-compliance. [PM-36 1.4.1]

Third party access granted to LSUS information systems that contain protected or restricted information is documented by a Business Associate Agreement or similar document that specifies the access to be granted and the controls to be used by both parties to ensure confidentiality, integrity, and availability of the data. [PM-36 3.2.3] For effective auditing and monitoring, all third party user accounts shall expire or be renewed no more than one year from the date they were created or renewed.

Any facilities management company engaged by LSUS shall be expected to comply with LSUS Computer Usage and Access policies and to execute a Business Associate Agreement or similar document that communicates the performance expected and the remedies available in the instance of non compliance. [PM-36 3.2.5]

LSUS' suppliers/vendors who handle protected or restricted information shall acknowledge compliance with the campus' information security procedures prior to the delivery of services. [PM-36 8.1.3]

LSUS shall require all third parties to execute non-disclosure agreements e.g. Business Associate Agreements when engaged in the use or disclosure of information classified as protected or restricted. [PM-36 8.1.4]

16.0 Notifications and Training

Please see LSUS Policy No. 3 18.00 which covers the LSUS Database Security Breach Notification process. [PM-36 1.6.2, 6.1.3, 9.1.2, 11.1.2, 11.2.1, 11.2.2]

Employees shall be informed of their regulatory responsibilities in relation to the use of computer based information and data. [PM-36 6.1.1] Regulatory responsibilities of employees in relation to use of computer based information should be included in any terms of employment.

Employees shall be informed of their obligation to comply with applicable copyright laws. [PM-36 6.1.2]

All LSUS campus temporary staff with access privileges to the campus networks shall acknowledge compliance with the campus' Computer Usage and Access Policy prior to beginning work with the campus. [PM-36 9.1.1]

Updates on Information Security awareness shall be provided to the staff on an evolving, ongoing basis as events warrant. [PM-36 9.1.2, 6.1.3]

Each LSUS campus faculty, staff, and student worker shall complete information security training appropriate for their job function by their appropriate supervisor. If the user's job responsibilities change, then the user's training requirements shall be reassessed and new training must occur, if required. [PM-36 9.2.1]

All new LSUS campus faculty, staff and students shall receive mandatory Information Security training appropriate for their job or educational function by their appropriate supervisor within thirty calendar days of their start date. [PM-36 9.2.2]

LSUS shall require an employee to acknowledge compliance with information security policies as it is applicable to their job duties. [PM-36 8.1.1] Employees shall be notified that non-compliance with information security policies can result in immediate disciplinary action, up to and including termination of employment and/or enrollment.

LSUS shall verify that new employees are eligible to participate in university business and its affiliated programs. [PM-36 8.1.2]

17.0 Disaster Recovery

For information on how LSUS and ITS handle disaster recover, please reference the Disaster Recovery Business Continuity Plan. [PM-36, 2.1.8, 3.2.4, 7.7.1 – 7.1.4]

AUTHORIZED: **___Mike Ferrell__________________** **_4/15/11_____**
Vice Chancellor for Business Affairs **Date**

APPROVED: **____Vincent J. Marsala_______ ____** **_4/15/11_____**
Chancellor **Date**