PM-36: Attachment 1
TABLE OF CONTENTS AND CHAPTERS 1-12

SECTION **PAGE**

SECTION PAGE

SECTION **PAGE**

I. Chapter 1—Securing Systems, Hardware, Software and Peripherals

A. Subunit 1—Purchasing and Installing Hardware

1. Policy Statement 1.1.1—Security Standards and Guidelines

Each LSU System campus shall develop and implement written technical standards to ensure the confidentiality, integrity, and availability of the data stored on its information systems. All equipment and software purchased or developed shall adhere to these standards. These standards shall be reviewed periodically.

2. Policy Statement 1.1.2 Specifying Information Security Requirements for New Systems

All proposed information systems to be purchased with LSU System campus funds (including donations, grants etc.) shall be submitted to the person designated by the IT department for review for adherence to IT department security standards, and approval prior to purchase.

3. Policy Statement 1.1.3—Installation, Upgrade and Testing of Hardware, Systems and Equipment

All hardware installations shall be planned and related parties impacted by the installation 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.

B. Subunit 2—Cabling, UPS, Printers, and Modems

1. Policy Statement 1.2.1—Supplying Continuous Power to Critical Equipment

All information systems identified as critical to LSU System campus operations shall be protected by an uninterruptible power supply adequate to provide continuity of services and/or orderly shutdown to preserve data integrity.

2. Policy Statement 1.2.2—Managing High Availability Systems

Each LSU System campus Information Technology department shall identify those systems which require a high degree of availability and ensure continued operation during power outages and hardware faults.

3. Policy Statement 1.2.3—Using Fax Machines/Fax Modems

Protected or restricted information shall only be faxed when more secure methods are not available.

4. Policy Statement 1.2.4—Using Modems/ISDN/DSL Connections

Protected or restricted information shall only be sent via non-LSU System campus network lines when more secure methods are not feasible. In that event, additional precautions e.g. encryption of data, virtual private network, etc., shall be employed to ensure against unauthorized interception and/or disclosure of protected information.

5. Policy Statement 1.2.5—Using Centralized, Networked, or Stand Alone Printers

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.

6. **Policy Statement—1.2.6—Securing Network Cabling**
All cabling in LSU System campus networks shall be secured to prevent unauthorized interception or damage.

C. Subunit 3—Consumables

1. **Policy Statement 1.3.1—Using Removable Storage Media Including Diskettes and CDs**
All protected or restricted information stored on removable media, including diskettes and CDs, 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 authorization from the campus designated official.

D. Subunit 4—Working Off Campus or Using Outsourced Processing

1. **Policy Statement 1.4.1—Contracting or Using Outsourced Processing**
Individuals responsible for commissioning outsourced computer processing of protected or restricted information shall ensure the services used are from companies that operate in accordance the campus' information security standards which 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.

2. **Policy Statement 1.4.2—Use of Laptop/Portable Computers, Portable Electronic Devices and the Removal of Equipment Off LSU System Campuses**
Laptops and other portable computing devices issued to LSU System campus employees shall not be used for activities unrelated to LSU 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 LSU System 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 patched in a timely fashion, and where applicable, anti-virus software with current virus data file (including spyware detection and firewalls) is installed and running continuously. In addition, only authorized personnel shall be permitted to take any equipment belonging to the LSU System campus off the premises and are responsible for its security at all times.

3. **Policy Statement 1.4.3—(Teleworking) or Working from Home or Other Off-Site Location**
LSU System campuses which allow teleworking or working from home shall establish procedures that ensure the confidentiality, integrity and availability of protected data accessed during any teleworking session.

E. Subunit 5—Hardware and System Documentation

1. **Policy Statement 1.5.1—Maintaining and Using Hardware and System Documentation**
Up to date hardware and system documentation, such as operator manuals or technical information provided by suppliers or vendors, shall be readily available to staff who are authorized to support or maintain the system.

F. Subunit 6—Other Hardware Issues

1. Policy Statement 1.6.1—Destruction and/or Reuse of Equipment

IT equipment and/or media owned by LSU System campuses shall only be disposed of by authorized personnel in accordance with the National Industrial Security Program Operations Manual (DOD standard 5220.22M) and the Louisiana Office of Information Technology policy. IT equipment and/or media owned by a LSU System campus 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 above standard prior to reassignment and/or reuse or disposal.

2. Policy Statement 1.6.2—Recording, Reporting and Correcting System Faults

Each campus shall develop and implement a procedure for documenting and responding to significant information system incidents that impact multiple users.

3. Policy Statement 1.6.3—Logon and Logoff from Computer

Logon procedures shall be strictly followed and users leaving their screen unattended must secure their workstation or logoff. All information systems storing protected or restricted information shall incorporate technical methods to secure unattended workstations in unsecured areas to prevent unauthorized use.

4. Policy Statement 1.6.4—Damage to Equipment

All deliberate damage to or theft of LSU System campus IT property shall be reported to the Security Officer and appropriate law enforcement as soon as it is discovered.

II. Chapter 2—Controlling Access to Information and Systems

A. Subunit 1—Controlling Access to Information and Systems

1. **Policy Statement 2.1.1—Managing Access Control Standards**
Each LSU System campus shall ensure that all access to information systems is based on the lowest level of privilege needed to perform one's job.

2. **Policy Statement 2.1.2—Managing User Access**
Access to any LSU System 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. When generic IDs are required by operational necessity, each campus shall develop procedures to prevent abuse. For audit purposes, such access, including the appropriate access rights or privileges, and a record of the authorization shall be maintained for six years after the access is terminated.

3. **Policy Statement 2.1.3—Securing Unattended Workstations**
Precautions shall be taken to prevent unauthorized changes to unattended equipment.

4. **Policy Statement 2.1.4—Managing Network Access Controls**
Access to LSU System campus information systems networks shall be strictly controlled to prevent unauthorized access. Each campus' IT department shall develop procedures and standards for securing network electronics against unauthorized tampering.

5. **Policy Statement 2.1.5—Managing Application Access Control**
The LSU System campus procedure for authorizing supervisor-level access shall require approval from the designated campus IT authority.

6. **Policy Statement 2.1.6—Managing Passwords**
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 on a periodic basis. The IT department of the LSU System campus shall develop and/or adopt standards for password length, password change interval and password complexity that are appropriate for the system being protected. These standards shall be reviewed periodically. These standards shall not be any less restrictive than that specified by the State of Louisiana Office of Information Technology policy.

7. **Policy Statement 2.1.7—Unauthorized Physical Access Security**
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.

8. **Policy Statement 2.1.8—Monitoring System Access and Use**
All LSU information systems that contain protected or restricted information shall be configured to log any and all information necessary to detect and record attempts of unauthorized access and system errors, to the extent that the logging facility exists and is capable. These logs with significant activity shall be examined in a timely fashion by staff determined as qualified by the campus IT department. Security incidents shall be reported to the Security Officer for appropriate action and follow up.

9. **Policy Statement 2.1.9—Managing System Access**
Access controls for information systems shall be set in accordance to the value and classification of the information assets being protected.

10. **Policy Statement 2.1.10—Controlling Remote User Access**
Each LSU System campus shall develop a procedure for authorizing remote access of LSU information systems by LSU faculty, staff, students and vendors. The campus IT department shall establish standards to ensure accurate authentication of remote users and the integrity and confidentiality of the information transmitted.

11. **Policy Statement 2.1.11—Emergency Access**
All LSU System campuses shall develop and implement a procedure to provide access to electronic information on an emergency basis (i.e., an employee is incapacitated and another employee must enter the system to continue his job function). For audit purposes, each instance of such access provision shall be documented and shall be maintained on file for a period of no less than six years, if the information accessed is protected information.

III. Chapter 3—Processing Information and Documents

A. Subunit 1—Networks

1. Policy Statement 3.1.1—Configuring Networks

All LSU System information system networks shall be designed and configured to deliver high availability, confidentiality, and integrity to meet business needs.

2. Policy Statement 3.1.2—Managing the Network

Each LSU System campus shall ensure that those responsible for managing the campus' network and preserving its integrity in collaboration with the individual system owners does so in accordance to the campus' IT department standards and job descriptions.

3. Policy Statement 3.1.3—Defending Network Information Against Malicious Attack

Each LSU System campus shall develop and implement 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 LSU network infrastructure. In the event that the system will not operate properly with the anti-virus software, appropriate information security safeguards shall be instituted.

B. Subunit 2—System Operations and Administration

1. Policy Statement 3.2.1—Appointing System Administrators

Each LSU System campus shall appoint systems administrators who demonstrate the qualifications established by the campus' IT department to manage the information technology systems and oversee the day to day security of these systems.

2. Policy Statement 3.2.2—Controlling Data Distribution

While appropriate data and information must be made available to authorized personnel when required, access to such data and information by all other persons shall be prohibited using appropriate technical controls.

3. Policy Statement 3.2.3—Permitting Third Party Access

Each LSU System campus shall develop and implement a procedure in which third party access granted to LSU System 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.

4. Policy Statement 3.2.4—Ensuring Information Integrity

All LSU System campuses shall develop and implement procedures to ensure that the integrity of electronic protected or restricted information is maintained in the event of processing errors, system failure, human errors, natural disasters and deliberate acts.

5. Policy Statement 3.2.5—Commissioning Facilities Management

Any facilities management company engaged by a LSU System campus shall be expected to comply with LSU System Information Security 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.

C. Subunit 3—E-mail and the World-wide Web

1. **Policy Statement 3.3.1—Downloading Files and Information From the Internet**
Each LSU System campus IT department shall develop standards and guidelines to ensure information, software and media downloaded from the Internet does not jeopardize its operations or the security of information systems.

2. **Policy Statement 3.3.2—Sending Electronic Mail (E-Mail) and/or Other Forms of Digital Communication**
Each LSU System campus shall develop procedures that require all email and/or any other form of digital communication generated by its information systems that contains protected or restricted information, including data attachments, shall only be permitted after confirming 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. In no case shall protected or restricted information be sent outside the LSU information infrastructure without taking precautions to ensure the confidentiality and integrity of the information.

3. **Policy Statement 3.3.3—Receiving Electronic Mail and/or Any Other Form of Digital Communication**
Each LSU System campus shall develop and implement standards and procedures that will ensure that malicious code is not delivered to or executed on LSU information systems by receiving email and/or any other form of digital communication.

4. **Policy Statement 3.3.4—Misdirected Information by E-Mail and/or Any Other Form of Digital Communication.**
Each LSU System campus shall develop and implement procedures that ensure that emails and/or any other form of digital communication that contain protected or restricted information, including attachments, are correctly addressed and only being sent to appropriate persons. This procedure shall include a mechanism in which the misdirected communication is correctly delivered without the content being viewed any further than is necessary to identify the appropriate recipient and deleted from the mistaken recipient's computer system.

5. **Policy Statement 3.3.5—Website Maintenance**
Each LSU System campus shall develop and implement a procedure which ensures LSU System websites that contain protected or restricted information are protected from unauthorized intrusion.

D. Subunit 4—Data Management

1. **Policy Statement 3.4.1—Transferring and Exchanging Data**
All restricted or protected information shall only be transferred outside of LSU networks, or copied to other media, when the confidentiality and integrity of the data can reasonably be assured.

2. **Policy Statement 3.4.2—Managing Data Storage**
All data stored on LSU information systems shall be managed to ensure the confidentiality, integrity and availability of the data.

E. Subunit 5—Backup, Recovery and Archiving

1. Policy Statement 3.5.1—Restarting or Recovering the System

All LSU information systems that contain protected or restricted information shall be protected by adequate backup and system recovery procedures. These procedures shall ensure the integrity of data files, especially when these files were replaced by more recent files.

IV. Chapter 4—Purchasing and Maintaining Commercial Software

A. Subunit 1—Purchasing and Installing Software

1. Policy Statement 4.1.1—Using Licensed Software

Each LSU System campus 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.

B. Subunit 2—Software Maintenance and Upgrade

1. Policy Statement 4.2.1—Supporting Application Software

All LSU 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.

2. Policy Statement 4.2.2—Disposing of Information System Software

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.

V. Chapter 5—Developing and Maintaining Custom Software

A. Subunit 1—Controlling Software Code

1. **Policy Statement 5.1.1—Managing Operational Program Libraries**
   Each LSU System campus shall implement a procedure in which only authorized staff may access operational program libraries.

2. **Policy Statement 5.1.2—Managing Program Source Libraries**
   Each LSU System campus shall implement a procedure in which only authorized staff may access program source libraries.

3. **Policy Statement 5.1.3—Controlling Deployment of Software Code During Software Development**
   All changes to systems, source code and operational program libraries shall be properly authorized and tested before moving to the live environment.

A. Subunit 2—Software Development

1. **Policy Statement 5.2.1—Software Development**
   Each LSU System campus shall implement a procedure in which all software developed for systems identified as critical to campus operations must always follow a formal managed development process appropriate for the size and scope of the system.

B. Subunit 3—Testing and Training Environments

1. **Policy Statement 5.3.1—The Use of Protected Data for Testing**
   Each LSU System campus shall implement a procedure that requires adequate controls for the security of protected or restricted data when used in the testing of new systems or system changes.

2. **Policy Statement 5.3.2—New System Training**
   Each LSU System campus shall implement a procedure in which users and technical staff are trained in the functionality and operations of all new systems.

VI. Chapter 6—Complying with Regulatory and Policy Requirements

A. Subunit 1—Complying with Regulatory Obligations

1. **Policy Statement 6.1.1— Awareness of Regulatory Obligations**
   All LSU System campuses shall develop and implement procedures to inform employees of their regulatory responsibilities in relation to the use of computer based information and data.

2. **Policy Statement 6.1.2—Copyright Compliance**
   All LSU System campuses shall develop and implement procedures to inform employees of their obligation to comply with applicable copyright laws.

3. **Policy Statement 6.1.3—Computer Misuse: Regulatory Safeguards**
   Each LSU System campus shall implement a procedure by which employees are informed of regulatory changes concerning computer misuse, as it directly impacts their job duties.

VII. Chapter 7—Business Continuity Planning

A. Subunit 1—Management of Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP)

1. **Policy Statement 7.1.1—Initiating the BCP/DRP**
Each LSU System campus shall develop and implement a written Business Continuity Plan (BCP) and/or Disaster Recovery Plan (DRP) to ensure the continuation of key information systems services in the event that these services are disrupted. A current copy of this Plan and any amendments shall be submitted to the LSU System Office of the Executive Vice-President for review and to be kept on file.

2. **Policy Statement 7.1.2—Assessing the BCP/DRP Security Risk**
Each LSU System campus shall conduct a formal risk assessment in order to determine the requirements for the BCP/DRP. Each LSU System campus shall review its risk assessment after each emergency and at least every three years.

3. **Policy Statement 7.1.3—Testing the BCP/DRP**
Each LSU System campus shall implement a procedure in which the BCP is tested at least annually. Results of such testing, i.e. a disaster recovery drill, shall be submitted to the LSU System Office of the Executive Vice President. The BCP/DRP shall be produced in the appropriate format to guarantee its availability during an emergency.

4. **Policy Statement 7.1.4—Training and Staff Awareness of the BCP/DRP**
All appropriate LSU staff shall receive training in the use of the BCP/DRP and in their continuity plan roles.

VIII Chapter 8—Addressing Personnel Issues Relating to Security

A. Subunit 1—Contractual Documentation

1. Policy Statement 8.1.1—Preparing Conditions of Employment

All LSU System campuses shall require employees to acknowledge compliance with information security policies as it is applicable to their job duties.

2. Policy Statement 8.1.2—Employing/Contracting New Staff

Each LSU System campus shall verify that new employees are eligible to participate in university business and its affiliated programs.

3. Policy Statement 8.1.3—External Suppliers/other Vendors Contracts

All LSU System campuses' suppliers/vendors who handle protected or restricted information shall acknowledge compliance with the campus' information security procedures prior to the delivery of services.

4. Policy Statement 8.1.4—Non-Disclosure Agreements

All LSU System campuses 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.

B. Subunit 2—Personnel Information Security Responsibilities

1. Policy Statement 8.2.1—Passwords and PIN Numbers

All LSU System campus faculty, staff and students are expected to treat passwords as private and highly confidential.

C. Subunit 3—Employment Termination

1. Policy Statement 8.3.1—Staff Resignations

All LSU System campuses shall ensure that the appropriate Security Officer is notified of all employee terminations and that access to LSU System 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 LSU System campus information, all access shall be terminated immediately.

2. Policy Statement 8.3.2—Procedures for Staff Leaving Employment

All LSU System campuses shall develop and implement a procedure to ensure that all LSU System campus property previously assigned to a departing employee is returned, and also that all keys, access cards and forms of employee identification are returned.

IX. Chapter 9—Training and Staff Awareness

A. Subunit 1—Awareness

1. Policy Statement 9.1.1—Awareness for Temporary Staff

All LSU System campus temporary staff with access privileges to the campus networks shall acknowledge compliance with the campus' Information Security policies prior to beginning work with the campus.

2. Policy Statement 9.1.2—Security Information Updates to Staff

Updates on Information Security awareness shall be provided to the staff on an evolving, ongoing basis as events warrant.

B. Subunit 2—Training

1. Policy Statement 9.2.1—Information Security Training on New Systems

Each LSU System campus faculty, staff and students shall complete information security training appropriate for their job function. If the user's job responsibilities change, then the user's training requirements shall be reassessed and new training must occur, if required.

2. Policy Statement 9.2.2—New LSU System Faculty, Staff and Student Training in Information Security

All new LSU System campus faculty, staff and students shall receive mandatory Information Security training appropriate for their job or educational function within thirty calendar days of their start date.

X. Chapter 10—Physical Security

A. Subunit 1—Campus Security

1. Policy Statement 10.1.1.—Preparing Campus for Placement of Computers

All LSU System campus information systems hardware and media that contain protected or restricted information shall be located in areas that are protected from physical intrusion, theft, fire, flood, excessive temperature/humidity or other hazards.

XI. Chapter 11— Protecting For, Detecting and Responding to Information Security Incidents

A. Subunit 1—Reporting Information Security Incidents

1. Policy Statement 11.1.1.—Defending Against Unauthorized or Criminal Activity
Each LSU system campus shall develop and implement procedures to defend campus networks and information systems that contain protected or restricted information against vandalism, unauthorized physical intrusion, unauthorized access, denial of service, virus attack, spyware/malware or criminal activity.

2. Policy Statement 11.1.2—Security Incident Procedures
All LSU system campuses shall develop and implement procedures requiring that all suspected or actual information security incidents as defined by the campus' IT department are promptly reported to the Information Security Officer or campus designee.

B. Subunit 2—Investigating Information Security Incidents

1. Policy Statement 11.2.1—Investigating the Cause and Impact of Information Security Incidents
All LSU system campuses shall develop and implement procedures for the thorough investigation of information security incidents as defined by the campus' IT department. Investigators shall be properly trained and qualified. Results of the investigation shall be thoroughly documented in a security incident report to be kept on file for at least six years. The report shall include any and all recommendations to prevent a recurrence of similar incidents.

2. Policy Statement 11.2.2—Responding to Information Security Incidents
All LSU System campuses shall develop and implement procedures for the response to information system security incidents as defined by the campus' IT department. Every effort shall be made to mitigate the adverse impact on the confidentiality, integrity and availability of data, and to preserve any evidence that could be used in the investigation of the incident.

XII. Chapter 12—Classifying Information and Data

A. Subunit 1—Setting Classification Standards

1. Policy Statement 12.1.1—Defining Information

All LSU System campuses shall maintain a database of their information assets to include rankings of each asset with regard to confidentiality, integrity, availability and criticality to operations.

2. Policy Statement 12.1.2—Classifying Information

Each LSU System campus shall adopt a method to classify its electronic protected or restricted information according to the level of confidentiality, sensitivity, value and criticality. This method shall not be less restrictive than the method defined by Louisiana state law and/or the State of Louisiana Office of Information Technology.

3. Policy Statement 12.1.3—Characteristics and Handling of Protected Information

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 LSU System 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 Security 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.

4. Policy Statement 12.1.4—Characteristics and Handling of Restricted Information

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 ongoing investigations, pending litigation, psychology notes and disciplinary action. All LSU System campuses shall take appropriate measures to ensure that restricted information is not disclosed to anyone other than to those individuals designated by management.

Best Practices Suggestions

In addition to the Policy Statements, the LSU System Information Security Plan Committee offers the following "best practices" suggestions to assist the campuses in complying with the regulatory information security mandates.

Best Practices Suggestions for Chapter 1, Section A, Subunit 1:

1. **Standards should be reviewed no less frequently than every 3 years and revised if necessary to ensure adherence to industry best practices. All standards documents should include version number and date of adoption for audit purposes. In the event that already existing systems do not meet the newly revised standards, then they may be grandfathered until a replacement or update can be planned and implemented.**

2. **The IT policy adherence review should be scalable to the size and complexity of the purchase. The campus IT department may at its own discretion set monetary and/or other parameters to determine appropriate levels of review and/or develop and publish a pre-approved list of items which are commonly purchased.**

Best Practices Suggestions for Chapter 1, Section B, Subunit 2:

1. **The sender of the protected or restricted information and the intended recipient should agree to the fax transmittal prior to sending.**

2. **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.**

3. **Each LSU System campus Information Technology department should establish standards for standards should be reviewed periodically, as with other IT department standards. This review should occur no less than once every 3 years and be revised if necessary to ensure the standards are in accordance with industry best practices. The campus IT department may, at its discretion "grandfather" older network installations, provided those installations were done in accordance with existing standards at the time of installation and/or good engineering practice, and the installation adequately serves the needs of the campus.**

4. **To prevent abuse of network facilities, all network connections should be monitored or secured.**

Best Practices Suggestions for Chapter 1, Section D, Subunit 4

1. **All protected or restricted information stored on a portable or mobile computing device should be encrypted.**

Best Practices Suggestions for Chapter 1, Section F, Subunit 6:

1. **Significant information system incidents should be corrected by qualified staff or third party technicians.**

2. **Equipment owned, leased or licensed by the LSU System campus should be supported by appropriate maintenance facilities and/or qualified engineers.**

Best Practices Suggestions for Chapter 2, Section 1, Subunit A

1. **Access records should be considered confidential and safeguarded as such.**

2. **Precautions to prevent tampering with workstations should include: limiting access to server rooms, locking wiring closets, incorporating idle time outs for work stations, and password controlled screensavers.**

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

4. **HIPAA Privacy reasonable safeguards pertaining to passwords should be included in password management standards where appropriate. The password management standard review should occur no less frequently than every three years and revised to incorporate advances in technology.**

5. **For effective auditing and monitoring, each campus should establish a threshold (or clipping level) to limit the amount of logging information generated.**

Best Practices Suggestions for Chapter 3, Section A, Subunit 1

1. **All anti-virus data files should be updated no less frequently than monthly.**

2. **All adequately tested operating system patches should be applied in a timely fashion.**

Best Practices Suggestions for Chapter 3, Section B, Subunit 2

1. **For effective auditing and monitoring, all third party user accounts should expire or be renewed no more than one year from the date they were created or renewed.**

2. **Systems' operations processes should be formally planned, authorized, scheduled and documented to ensure that necessary processes are successfully run and completed, and that unauthorized processes are not performed. Changes to routine systems operations should be fully tested and approved before being implemented.**

3. **In order to accurately document and mitigate information security incidents, all LSU campus information system clocks should be synchronized regularly to the extent possible.**

4. **Only qualified staff or third party technicians should repair information system hardware faults.**

5. **If possible, transaction and processing reports should 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.**

Best Practices Suggestions for Chapter 3, Section C, Subunit 3

1. **Only personnel who demonstrate the qualifications established by the campus IT department should modify the campus website, especially if it contains protected information. These modifications should be documented for audit purposes**

Best Practices Suggestions for Chapter 4, Section B, Subunit 2

1. **Each LSU System campus should implement a procedure in which patches to resolve software bugs are only applied when verified and authorized by the campus IT department.**

2. **Each LSU System campus should develop and implement a procedure in which system faults are recorded and reported to those responsible for system support/maintenance.**

Best Practices for Chapter 5, Section A, Subunit 1

1. **Amendments to operational program libraries should only be made using a combination of technical access controls and strong procedures operated under dual control.**

2. **Amendments to program source libraries should only be made using a combination of technical access controls and strong procedures operated under dual control.**

Best Practices Suggestions for Chapter 5, Section B, Subunit 2

1. **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.**

2. **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 should be assigned to the business owner of the system.**

3. **Each LSU System campus should implement a procedure in which proper segregation of duties should be ensured for all areas dealing with system development, system operation, or system administration.**

Best Practices Suggestions for Chapter 5, Section C, Subunit 3

1. **Each LSU system campus should maintain a suitable test environment for all systems identified as critical to campus operations.**

2. **Each LSU System campus should implement a procedure in which new systems are tested for capacity, peak loading, and stress testing. The new system should demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the campus.**

3. **Normal system testing procedures for each LSU System campus should incorporate a period of parallel running, when deemed necessary, prior to the new or amended system being acceptable for use in the live environment.**

Best Practices Suggestions for Chapter 5 in General

1. **Each LSU System campus should implement a procedure in which all new and enhanced systems are fully supported by comprehensive and recent documentation. New or upgraded systems should not be introduced into the live environment unless supporting documentation is available.**

2. **Each LSU System campus should ensure that all vendor developed software meets the User Requirements Specifications and offers appropriate product support.**

Best Practices Suggestions for Chapter 6

1. **Regulatory responsibilities of employees in relation to use of computer based information should be included in any "Terms of Employment" and the campus' Code of Conduct.**

Best Practices Suggestions for Chapter 8, Section A, Subunit 1

1. **Compliance with information security policies should be included in any "Terms of Employment" and the Campus' Code of Conduct.**

2. **Lending of keys, both physical and electronic, should be prohibited by each LSU System campus. 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.**

3. **Employees should 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.**

Best Practices Suggestion for Chapter 10

Each LSU System campuses should develop and implement processes to record the identity of individuals who improperly gain physical access to secure information technology areas.

Best Practices Suggestions for Chapter 11, Section A, Subunit 1

1. **Each LSU system campus should adhere to industry recognized best practices when collecting and protecting evidence from information systems so that criminal perpetrators can be prosecuted to the fullest extent of the law.**

Best Practices Suggestions for Chapter 12

1. **At a minimum, the classification system should incorporate four levels. Examples of these levels are, in increasing order of restrictions, Public, Internal, Protected and Restricted.**

2. **Public information can be defined as information with no restrictions and can be released to the general public in accordance with university policy.**

3. **Internal information can be defined as information regarding the internal business and education operations of the LSU System and its campuses. 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 LSU System campus.**