LSU HCSD HIPAA Security Policy PM 36

Hospital and Information Technology Departments
Procedure Manual

Table of Contents

INTRODUCTION

The purpose of this document is to provide the procedures for the HCSD hospitals to meet the mandates of the Louisiana State University System Information Security Plan, (PM36).

Most hospitals have a tiered policy and procedure system. Administrative policies comprise the hospital-wide or interdepartmental directives while there are departmental based policies for intradepartmental subjects. This document was written using this scheme.

PROCEDURES

Chapter 1—Securing Systems, Hardware, Software and Peripherals

Subunit 1—Purchasing and Installing Hardware

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.

All HCSD facilities shall adhere to:

1. The Office of Information Technology (OIT) standards[1] found at http://www.state.la.us/oit/standards/index.htm
2. The LSUHSC-NO Enterprise Information Security (EIS) Workstation and Server Standards and Application Requirements (See Appendix)
3. The LSUHSC-NO Enterprise Networking Wiring Standards (See Appendix)
4. Any additional standards set at the facility or HCSD HQ that are more restrictive than the above

All local standards shall be reviewed on an annual basis with a review date to be specified in the standards.

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.

1. All IT projects shall be reviewed by the local IT Director/IT Security Lead prior to purchase or implementation.
2. All IT systems that contain protected and/or restricted data shall be reviewed by the IT Security Lead and must:
   2.1. Adhere to the Server Security Standards in Appendix A
   2.2. Adhere to the Application Security Requirements in Appendix C
   2.3. Be submitted to Enterprise Information Security (EIS) to ensure compliance with HIPAA and other regulatory entities.

[1] Louisiana Revised Statute 39:15.1

I. APPLICABILITY

1. OIT Definition/Example of an IT Project

1.1. Examples of IT project/initiatives are: system development projects, software acquisition and installation, hardware acquisition and installation, operating and/or host services contracts, consulting services contracts, enhancements and upgrades to existing systems, telecommunications services, IT training.

1.2. OIT does not require approval of systems that use IT to provide a solution but are not inherently IT projects. Examples not considered IT projects by OIT are: systems that provide "direct patient care" such as to treat a patient with radiation therapy or monitor vital signs, projects that provide a service but use IT such as the Maryland Hospital Association (MHA), or those that provide in-service and use IT.

2. Review Process

2.1. If an IT project has an impact on the HCSD or LSUHSC enterprise then notifications of IT demonstrations, evaluations, site visits, etc should be sent to the "HCSD IT Security Leads" email distribution list whose members will be responsible for distribution within each IT Director's/IT Security Lead's area of responsibility for request for comment or request for participation.

2.2. The IT Director/IT Security Lead shall validate his/her assessment that the IT project meets the IT security standards of the organization through LSUHSC Enterprise Information Security (EIS) before proceeding.

2.3. IT projects that meet any of the criteria below should be reviewed by the HCSD Director of IT/HCSD HIPAA IT Security Officer.

2.3.1. Criteria for Review and Notification at HCSD Level

2.3.1.1. IT project that requires OIT or PST approval
2.3.1.2. IT project that substantially increases WAN traffic
2.3.1.3. IT project that requires modifications or expansion of the existing LAN other than additional client access points
2.3.1.4. IT project that includes IT purchases for more than one hospital
2.3.1.5. IT system that requires an interface to other LSUHSC-NO or HCSD resources
2.3.1.6. IT project that will be purchased with HCSD-HQ funds
2.3.1.7. IT project that requires LSUHSC-NO or HCSD enterprise resources

II. GENERAL PROCEDURE GUIDELINES

The following guidelines provide sets of questions to assist in the IT project planning process where applicable.

1. Financial
   - 1.1. Is there a source of funds?
   - 1.2. What is the estimated cost of the project?
   - 1.3. What are the ongoing costs for software and hardware maintenance?
   - 1.4. Are upgrades included in the software maintenance costs?
   - 1.5. Will the project enhance revenue and if so how?
   - 1.6. Do the reporting capabilities and data elements meet the needs of HCSD cost reporting, general ledger, banking, etc?
   - 1.7. What are the benefits of a system-wide purchase/implementation?
   - 1.8. Is the project an upgrade to an existing system?
2. Managerial
   - 2.1. Who is/are the executive sponsor(s)?
   - 2.2. Who is/are the project leader(s)?
   - 2.3. Who is on the project team and what are each member's responsibilities?
   - 2.4. What is the priority of the project?
   - 2.5. Are there any conflicting projects?
   - 2.6. Is the project hospital-specific or system-wide?
   - 2.7. What is the timeline?
   - 2.8. Is OIT approval required? (Total project cost is > $100,000 over 5 years)
   - 2.9. Is a competitive process required? (Software purchase price > $100,000, Hardware > $1,000 and not on State Contract)
   - 2.10. Is PST required? (Software purchase price > $100,000)
   - 2.11. Is Board of Supervisors approval required (all billing and academic applications > $100,000 or use judgment that the application will have a significant fiscal or policy impact on HCSD)
   - 2.12. Is the funding for this project coming from a grant? Are there special stipulations placed on the use of the application or hardware?
3. Stakeholders
   - 3.1. Who are the stakeholders, do they know about the project, and how are they affected?
     - 3.1.1. Administrative -
     - 3.1.2. Clinical –
     - 3.1.3. Financial –
     - 3.1.4. IT –
     - 3.1.5. Functional –
     - 3.1.6. Compliance –
     - 3.1.7. Patient -
4. Operational
   - 4.1. POSSIBLE vendor questions:
     - 4.1.1. What is the underlying architecture of the application?
     - 4.1.2. What interfaces are needed and what are the specifications?
     - 4.1.3. What are the network requirements?
     - 4.1.4. What are the hardware specifications?
     - 4.1.5. What are the storage needs?

4.1.6. What are the training needs?
4.1.7. Does the system comply with the EIS workstation, server, network, and application security standards?
4.1.8. Are the data requirements sufficient for interfacing to standard applications such as DSS?
4.1.9. Are the data requirements sufficient for cost reporting?
4.1.10. Will the vendor need access to onsite servers?
4.1.11. If applicable, give verifiable references of current customers with interfaces to (choose all that apply):
4.1.11.1. Siemens Invision Billing, Order Entry and ADT.
4.1.11.2. MISYS Lab System
4.1.11.3. Pharmacy System
4.1.11.4. Etc.

4.2. Can the vendor provide studies showing benefits/savings to their current customers?
4.3. What is the scope of the project?
4.4. What is the goal of the project?
4.5. Who will be the users of the project?
4.6. Has a site survey been performed of the area by the enterprise network group to determine the feasibility and cost of implementing wired/wireless in the chosen location?
4.7. Who will implement the application?
4.8. Who will administer the application after implementation?
4.9. Who will implement the hardware?
4.10. Who will administer the hardware after implementation?
4.11. Who will implement the network?
4.12. Who will administer the network after implementation?
4.13. What additional duties will exist for whom once the project is implemented?
4.14. Have all responsibilities for the application been documented (Hardware, OS, Software, Data Entry Process, Billing, …)

5. Compliance
   5.1. HIPAA – Does the IT project comply with HIPAA and other Federal or State regulations?
   5.2. Is the project required in order to meet Federal or Regulatory Compliance?
   5.3. Is the project compliant with federal mandates and proposed federal mandates or reporting?
6. Clinical
   6.1. Has the vendor implemented this product at a facility or system like ours and can they guarantee a smooth transition to the new application with no disruption of patient care?
   6.2. What are the positive and negative impacts to patient care?
   6.3. What are the positive and negative impacts to clinician treatment time?
   6.4. How will this application affect wait times?
   6.5. How will this application improve patient safety?
   6.6. How will this application improve the quality of patient care?
   6.7. How will this application advance patient education?
   6.8. Will the system improve customer satisfaction and how?

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.

Procedure

1. Any significant system change that has the likely or expected potential to affect a user group shall be planned with the knowledge and cooperation of that group.
2. A significant system change is any change to hardware, software, or communications lines that has the potential to affect the availability or integrity of a program or its data.
3. To meet the criteria of "likely" or "expected," the change could have documentation of known faults, be provided untested by the vendor, being applied to a program that has local customizations that could not be tested by the vendor, or an extended downtime may be needed for the change.
4. Certain trusted changes such as virus protection updates and operating system patches that are routinely released by the original software vendor can be applied to workstations and file servers of non-critical applications without extended testing.
5. Any system that contains restricted or protected information should be backed up with a restore point prior to implementing the change.
6. All change actions should be weighed against the potential outcome of not making the change.
7. Critical software updates for known vulnerabilities may take precedent over a group's productivity.
8. Protecting the program and data is always the top priority.
9. All significant changes to a system should be documented with the change and the date it occurred.

Subunit 2—Cabling, UPS, Printers, and Modems

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.

Procedure

1. Selection of equipment for support by uninterruptible power supply shall be based on the critical equipment inventory.
2. For data storage devices the uninterruptible power supply should be connected to computing device for orderly shutdown in a backup power supply system failure.
3. Uninterruptible power supplies shall be maintained and tested according to manufactures recommendations.

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.

Procedure

Each HCSD facility shall review and update their list of critical applications on an annual basis. Applications deemed critical must be included in the local DRP. Any application installed that will be deemed critical must be protected by UPS and emergency power. HCSD has a comprehensive risk assessment that includes an inventory of all applications and ranks them by criticality.

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

Procedure

The sender of the protected or restricted information and the intended recipient shall agree to the fax transmittal prior to sending

Documents with personal identifiers can only be faxed with appropriate safeguards. A list of medical record numbers without other personal identifiers may be faxed, providing there is no reference to medical conditions on either the faxed copy or the cover sheet. Users are responsible for ensuring that faxes are not left on the fax machine.

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.

EIS 100 Procedure

In the event that protected or restricted information cannot be sent via LSUHSC-NO network lines, 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.

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.

Covered by ROI HIPAA Security training.

Policy Statement 1.2.6 Securing Network Cabling

All cabling in LSU System campus networks shall be secured to prevent unauthorized interception or damage.

See Enterprise Networking Standards in Appendix.

Subunit 3—Consumables

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.

Procedure

The use of removable media to transport protected or restricted media is strongly discouraged. Specific administrative approval is required for the removal of protected information from the campus when stored on removable media. The user should obtain electronic or written documentation of the approval from the appropriate department director.

1.1. All diskettes, CDs and other storage media that contain confidential information that has not been completely de-identified:
   1.1.1. shall include only the minimum amount of information necessary to accomplish tasks assigned by the person's supervisor,
   1.1.2. shall be encrypted and stored in locked container(s) when not in use,
   1.1.3. shall be "wiped" or destroyed, not just erased, immediately upon completion of the assigned task
   1.1.4. shall require local agency administrative approval, and shall never be taken into the field unless encrypted.

Subunit 4—Working Off Campus or Using Outsourced Processing

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.

The BAA can be found on page 29 of
http://www.lsuhsc.edu/hcsd/policies/Public/Attachments/PM-36.pdf

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.

Procedure

1.1. The IT Director at each facility or designee shall keep a listing of all portable computing devices (PCD) and who is in possession of the device. Any change in the possession of the portable computing device shall be reported to the IT Director immediately.

1.2. Each employee with a PCD shall have appropriate approval stating the need for the device prior to possession. The employee shall sign an LSU Portable Computing Device Release prior to using the device.

1.3. Handling and Storage of Laptops

1.3.1. Safety and security of the PCD is the responsibility of the employee that it is assigned to.

1.3.2. PCD's are stored in a secure, locked location within the office when not in use. Confidential information on PCD removable drives should be carried in a secure vessel. If possible the media containing the confidential, encrypted data should be locked in a location apart from the laptop when not in use.

1.3.3. During necessary travel, laptops shall be stored in a locked auto trunk or, if a trunk is not available, in a location not visible from outside the vehicle. In hotels, laptops should be stored with hotel security when the employee is not in the room.

1.3.4. LSU is not responsible for any injuries, damages, claims, including legal expanses, incurred by the user caused by the transportation, selection, possession, ownership, maintenance, condition, and operation of the portable computing device. The user agrees to reimburse and defend LSU against any claims for such losses, damages, claims or expenses. This indemnity continues after the use period expires for acts or omissions, which occurred during the use period.

1.3.5. Loss of any PCD shall be reported immediately to the IT Director/IT Security Lead of the site.

Sample Portable Computing Device Release Form

LSU HCSD Portable Computing Device Use Agreement

As the user of a portable computing device owned/supplied by a Louisiana State University entity you agree to the following provisions:

I. **Obligations**
Once the term if this Use Agreement has begun, your commitments become irrevocable and nontransferable.

II. **Responsibility**
It is the employee's responsibility to take appropriate precautions to prevent damage to or loss/theft of your portable computing device. The employee or department may be responsible for certain costs to repair or replace the PCD if the damage or loss is due to negligence or intentional misconduct. Policies for appropriate use of state/LSU property as identified by LSU HCSD policy or elsewhere may be used to determine whether liability due to negligent behavior exists.

III. **Theft**
If the PCD is lost or stolen it must be reported to the agency's IT Director and the agency police immediately. For theft or loss off campus, it should also be reported to local police. The police report should include the serial number for the lost PCD. A copy of the police report must be sent to Information Technology within 48 hours of the discovery of the loss. Failure to secure and submit a police report could result in personal liability for replacement cost.

IV. **Upgrades and Troubleshooting**
Should a PCD require hardware upgrade (e.g., memory, peripheral, or hard disk), software installation, or have problems that cannot be resolved over the telephone, the PCD will need to be brought to the agency for hardware service, software installation, or problem diagnosis. Information Technology staff will not visit your home or go to off-campus locations to provide services.

V. **Software Licensing**
The PCD will be configured with a standard suite of programs that are appropriate for the type of computer you received based upon the campus software standards. It is also possible that other applications will be provided to you by the agency, based upon your professional needs or the requirements of the PCD. LSU has policies for appropriate use of software, including the requirement to demonstrate legal license to a program before it can be installed on an LSU owned PCD. Users will not in general be given administrative rights to the PCD they use, whether the computer is a desktop or a PCD. You may not load games, entertainment software, or personal finance software on an LSU owned PCD computer.

VI. **Backup**
You are responsible for maintaining an appropriate backup of your PCD, especially of the work-related documents and data files you create that are not restored when reinstalling the operating system and programs. Depending upon how you intend to use the PCD, you may need to store some of your documents and data files on the PCD's hard disk drive. It would be prudent to establish a process of copying the data files you use on the PCD to your central data storage area as an added precaution against data loss. You should not use central data storage to backup personal documents or data files.

VII. **Virus, Hacking, and Security Protection**
To ensure that virus protection and other security patches are current, PCDs must be connected to the LSU network on a regular basis and users must take responsibility for ensuring that security updates take place on PCDs in their care. In the case of a significant security alert, users may be contacted by e-mail and/or voicemail, to bring in their PCDs to the helpdesk to ensure proper security is enabled on the PCD. Although Information Technology pushes updates to agency computers, PCD's that are frequently off the network may require manual updating.

VIII. **Indemnity**
LSU is not responsible for any injuries, damages, claims, including legal expanses, incurred by the user caused by the transportation, selection, possession, ownership, maintenance, condition,

and operation of the portable computing device. The user agrees to reimburse and defend LSU against any claims for such losses, damages, claims or expenses. This indemnity continues after the use period expires for acts or omissions, which occurred during the use period

By my signature below, I state that I have been given a copy of this use agreement and will abide by it and by all applicable federal, state, and university laws and regulations in the use of the assigned portable computing device.

_____ _____

Signature Date

_____

Printed Name

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.

Procedure

1) When using a desktop computer from home or when traveling the screen should be placed so it not visible to non-authorized personnel walking by the office or through a hallway. Additionally, computer screens should be situated so that they are not visible through windows.
2) When laptop computers are used, the screens are managed so as to prevent viewing by others. The laptop is never out of sight of the employee when not secured.
3) All teleworking sessions require a virtual private network (VPN) connection, a Citrix Desktop connection, or a dialup connection through an enterprise RAS solution

Subunit 5—Hardware and System Documentation

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.

Subunit 6—Other Hardware Issues

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.

Procedure

Any HCSD computing equipment possessing media with protected or restricted information shall have the media wiped of all information in accordance with the state Office of Information Technology specifications, (DoD 5220.22M). Destruction of the media is an option if wiping of the media cannot be assured.

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.

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.

See Incident Response Procedure next page.

D.1 Information Security Incident Response Procedure

An information security incident is any use or attempted use of LSUHSC-NO information technology assets in violation of Federal or State laws or regulations or University policies. Information security incidents can be categorized as follows:

D.1.1 External Security Incidents – Originating from outside the LSUHSC-NO network.

i. Unauthorized access – An individual or group gains or attempts to gain access to the LSUHSC-NO network in order to obtain information or to control systems.
ii. Denial of Service – An individual or group coordinates Internet traffic directed at the LSUHSC-NO network such that legitimate use of the network is adversely impacted or impossible.
iii. Malware – This covers a variety of software including viruses, trojans, and spyware which are installed on systems without the user's knowledge and can adversely impact the availability of the network and compromise the security of protected information.

D.1.2 Internal Security Incidents – Incidents committed by LSUHSC-NO and HCSD faculty, staff, students, or external users.

i. Unauthorized access – An individual gains or attempts to gain access to information he or she is not permitted to see.
ii. Unauthorized use – Use of LSUHSC-NO and HCSD information technology assets in violation of Federal or State laws or regulations or University policies by a faculty or staff member, student, or external user.
iii. Criminal use – Use of any information technology asset, whether University or personally owned, on the University premises or via the LSUHSC-NO network, which violates Federal or State law.

D.1.3 Computer Services Incident Response Team

The Enterprise Information Security Group will maintain an Incident Response Team (CSIRT). The team will consist of:

1.3.6. Enterprise Information Security Manager (Chair)
1.3.7. Emergency Response Team (Enterprise Information Security)
1.3.8. IT Security Lead at location of Incident
1.3.9. Internal Counsel
1.3.10. Compliance Officer at location of incident
1.3.11. HCSD Specific – Each HCSD site shall create an email notification list consisting of the CSIRT specific to their location
  1.3.11.1. HCSD Director of Compliance
  1.3.11.2. HCSD IT Security Officer/IT Director

D.1.4 Emergency Response Team (ERT)

The ERT operates under the direction of the CSIRT Chair and functions as the first responders when an elevated or severe security incident is discovered or reported. The ERT will be comprised of all members of the Enterprise Information Security Group. At least one member of the ERT is on call at all times, is available to respond to a report of a

security incident and has the contact information of the other ERT and CSIRT members should assistance be needed.

D.1.5 Incident Response Preparation

The following steps have been taken in preparation to respond to a security incident.

1.3.11.3. All faculty, staff, and students are required to take training to recognize potential security incidents and report them to the Help Desk or their computer supporter.

1.3.11.4. A firewall has been installed between the LSUHSC-NO network and external networks.

1.3.11.5. The LSUHSC-NO Office of Compliance Programs has developed a computer forensic analysis capability.

1.3.11.6. All workstations and servers are equipped with anti-virus software which is updated automatically and anti-spyware software.

1.3.11.7. All operating systems patches are pulled from workstations to ensure patch levels are up-to-date.

1.3.11.8. Clocks on all host systems are synchronized.

D.1.6 Incident Response Detection Notification and Analysis

Detection of a security incident may occur in one of several ways:

i. Report to the Help Desk.
ii. Report to a Computer Supporter.
iii. Report from outside agency.
iv. Alert from monitoring software (Antivirus, IDS, etc.)
v. Review of system logs.
vi. Internet monitoring reveals inappropriate use.
vii. Malfunction.

D.1.7 Security Incident Matrix

Once a security incident has been detected or suspected, the security incident classification and reporting matrices (Table D-1 and D-2) are consulted to determine the appropriate action for handling of the incident. If it has been deemed necessary to notify the ERT during normal working hours, a call is placed to the Enterprise Information Security Group. After hours, the ERT member on call is paged. The ERT begins the analysis of the incident which will form the basis of containment actions.

i. Begin a log of all facts uncovered and all activities undertaken.
ii. Collect and analyze data to determine the nature of the incident and develop a containment strategy.
iii. Notify CSIRT Chair. (CSIRT Chair may make other notifications as deemed necessary.)
iv. Depending on the severity of the incident also notify the HCSD IT Security Officer/HCSD IT Director who will in turn notify the HCSD Director of Compliance, HCSD CEO, HCSD Deputy CEO, and HCSD CMO if appropriate.

D.1.8 Containment, Eradication, and Recovery

A. Priorities - In responding to a security incident, the CSIRT will observe the following priorities:
    i. Human life and safety.
    ii. Confidentiality and integrity of protected information.
    iii. Re-establishment of essential systems.
    iv. Preservation of evidence for possible prosecution and/or sanction.
    v. Re-establishment of non-essential systems.

B. The containment strategy is implemented
    i. Users are kept up-to-date with expectations as appropriate.
    ii. Affected systems are isolated and countermeasures applied.

C. Evidence collection (N.B.: Evidence is collected under the direction of the Compliance Officer at the location of the incident.)
    i. Compromised systems or systems believed to contain evidence are isolated from the network but not shut down.
    ii. The Compliance Officer at the location of the incident is contacted for further direction in the collection of evidence.
    iii. If LSUHSC and/or HCSD faculty, staff, student, or external user is suspected as a perpetrator, the following additional data is collected:
        a. The files in the User's O: drive
        b. The messages in the User's email mailbox.
    iv. If criminal activity is suspected, the following additional steps are taken:
        a. Most recent Exchange backup containing User's mailbox is removed from backup rotation and secured.
        b. Most recent file backup containing User's O: drive is removed backup rotation and secured.
        c. System logs are preserved and secured.

D. Recovery steps
    i. Remove inappropriate and/or unauthorized material.
    ii. Cut off unauthorized access.
    iii. Restore data from backups.

D.1.9 Post Incident Review, Lessons Learned Session, and Report

i. Review incident logs.
ii. Identify what worked.
iii. Identify what did not work.
iv. Develop recommendations to address deficiencies
v. Write report.

Table D-1: Information Security Incident Reporting Matrix

	Level 1 Incidents	Level 2 Incidents	Level 3 Incidents
	Guarded	**Elevated**	**Severe**
Report Frequency	Upon completion of initial investigation and upon resolution. Monthly status report submitted to CSIRT every 30 days.	Upon recognition of occurrence. Subsequent reports at least weekly or as requested and until resolved.	Upon recognition of occurrence and subsequent reports at least daily or as requested.
Report To	10. IT Security Lead at location of incident 11. CSIRT Chair	12. IT Security Lead at location of incident and HCSD IT Security Officer 13. CSIRT	14. IT Security Lead at location of incident and HCSD IT Security Officer 15. CSIRT

Table D-2: Information Security Incident Classification Matrix

	Level 1 Guarded	Level 2 Elevated	Level 3 Severe
Impact	• Minor Impact on Operations. • Information is received concerning threats to which the LSUHSC-NO Information Systems are vulnerable. • An IT resource has been stolen or lost containing information classified above Unrestricted.	• Moderate impact on operations. • Business Continuity at risk or affected. • Believed threat of an imminent attack. • An IT resource has been stolen or lost containing information classified above Operational. • Potential long-term negative effect on the institution. • Potential substantial negative financial impact or loss of public confidence.	• Severe impact on operations. • Business continuity is disrupted. • Long-term negative effect on the institution. • Likely Substantial negative financial impact or loss of public confidence.
People	• A physical intrusion has been detected. • Abuse of User Privileges. • Physical security suspect. • Local information security policies and procedures have been violated.	• Identified risk for personal harm or safety. • A physical intrusion to secured locations has been detected. • Potential for personal harm. • Abuse of access to IT resources above user level. • Isolated case of suspected or confirmed identity theft.	• Personal security or safety has been compromised. • Personnel have been harmed. • Multiple instances of suspected or confirmed identity theft.

Data (Either in Transmission or at rest)	Data classified Unrestricted or Operational: Availability affected. Unauthorized access or requests for access. Integrity violated. Little or no loss of data. Confidentiality suspect or compromised. Vulnerable to a known exploit. Availability of systems affected Potential for penetration detected. Denial of service attack(s) with no impact on operations System probes, scans, and/or similar activities are detected on IT resources. Instances of known computer viruses and/or worms are detected easily and	Data classified as Critical or above: Availability affected. Unauthorized access or requests for access. Integrity violated. Loss of data. Risk for or unauthorized disclosure. Confidentiality suspect or compromised. Widespread instances of known viruses and/or worms, not handled by deployed anti virus or other installed software. Penetration attempts detected with impact on operations Denial of service attack(s) with impact on operations Significant number of systems affected.	Data classified as Restricted: Availability lost. Unauthorized access or requests for access. Integrity violated. Loss of data. Unauthorized disclosure. Confidentiality suspect or compromised. Penetration detected with significant impact on operations. Widespread number of systems affected. Loss of mission critical systems or mission critical applications. Contain content in violation of federal and/or State law.

	handled by deployed anti virus or other installed software.	System Integrity compromised
Systems	Unauthorized access suspected.	Loss of (non critical) systems or applications
	Vulnerable to a known exploit.	Contain content in violation of LSUHSC-NO policies
	Incidental unsuccessful access	

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.

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.

Chapter 2—Controlling Access to Information and Systems

Subunit 1 Controlling Access to Information and Systems

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.

EIS 100

Access to application supervisor-level commands shall require authorization from the employee's supervisor and/or the owner of the application. Access to operating system supervisor and/or administrator commands shall be restricted to those persons who are authorized to perform systems administration/management functions.

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.

EIS 100

C.2 Generic Accounts

Generic accounts are used to provide access to LSUHSC-NO network resources for third-party software supporters, contractors, or LSUHSC-NO computer supporters that need application service accounts.

C.2.1 Acquiring a Generic Account

The owner of the resource (the LSUHSC-NO contact) will notify Enterprise Information Security via email that a vendor, contractor, or computer supporter will need a generic account to access the network. Before creating the account, LSUHSC-NO shall determine the method to allow access into the LSUHSC-NO network. This may require discussions between the vendor, LSUHSC-NO contact, and the firewall administrator. If it has been decided that a generic account is required, the account will be set up according to Enterprise Information Security procedures.

C.2.2 Vendor Account Requirements
Vendors and contractors must submit a vendor account policy which contains a vendor account agreement (C.2.4) before being given access to the LSUHSC-NO network. These policies are kept on file by the Enterprise Information Security group.

C.2.3 Enabling a Generic Account
Activation of generic accounts must be authorized by the LSUHSC-NO contact. The default activation period is 24 hours unless requested otherwise. Prolonged activation periods must be justified. When a generic account is activated, an email must be sent to the LSUHSC-NO contact notifying them of the new expiration date.

C.2.4 Generic Account Agreement for Vendors
a) I acknowledge that I am responsible for all activity attributable to the account assigned to my organization.
b) I will use my organization's account to perform authorized activities only (i.e., to carry out contract-related responsibilities).
c) If I abuse or gain unauthorized access to computer resources, I understand that LSUHSC may immediately revoke my account and report my conduct to law enforcement authorities.
d) I understand that, upon change or termination of my organization's relationship with LSUHSC, my organization's access to resources on the LSUHSC network will be reviewed and modified or terminated as appropriate.
e) I understand the importance of privacy and confidentiality of information and in particular patient information, student records, and employee personal data. I pledge to handle all sensitive data I access with the appropriate care and precautions.
f) I will abide by CM-42, the University policy regarding appropriate use of its network infrastructure. The policy can be found at
http://www.lsuhsc.edu/no/administration/cm/cm-42.htm.
g) I have verified that my company has a Business Associate
Contract on file with LSUHS

Policy Statement 2.1.3—Securing Unattended Workstations

Precautions shall be taken to prevent tampering of unattended equipment by unauthorized persons.

Procedure

1. All workstations should be placed in a secured location.
   1.1. In locations that are not at all times occupied and cannot be secured the PC should be secured to the work area.
2. Viewing screens should be located so that unauthorized personnel cannot view the information on the screen.
   2.1. Where it is impossible to protect the peripheral view of the screen privacy filters shall be employed.
3. Private or restricted information shall not be stored on a computer in a public use or untenable area.

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.

EIS 100

Access to LSUHSC-NO information systems networks shall be strictly controlled to prevent unauthorized access. The Office of Computer Services network equipment standards (current standards attached) shall be utilized to secure network electronics against unauthorized tampering.

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.

EIS 100

Access to application supervisor-level commands shall require authorization from the employee's supervisor and/or the owner of the application. Access to operating system supervisor and/or administrator commands shall be restricted to those persons who are authorized to perform systems administration/management functions.

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.

EIS 100

All LSUHSC-NO computer accounts must be password protected in accordance with LSUHSC-NO password policy. This policy shall not be any less restrictive than the Louisiana Office of Information Technology password policy (IT STD-009). These password standards shall be reviewed no less frequently than every three years and revised to incorporate advances in technology.

The LSUHSC-NO Password Policy requires that:
C.3.1 Minimum password length and format shall be no less than eight (8) characters.
C.3.2 Minimum password complexity should contain at least 3 of the 4 categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and non-alphanumeric characters (%,&,!).
C.3.3 Maximum validity periods for passwords to be no greater than 30 days, with specific exemptions granted for special purposes such as enabling a stored procedure to run against a database.

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.

EIS 100

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.

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.

EIS 100

All LSUHSC-NO 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 Office of Enterprise Computer Services. Reporting of suspected security incidents shall follow the process defined in the Information Security Response Procedure (see Policy Statement 1.6.2 above).

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.

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.

EIS 100

All methods for accessing the LSUHSC-NO network remotely shall use encryption and network account authentication to ensure the confidentiality, integrity, and availability of information transmitted during any session. All remote access shall be approved by the user's supervisor in conjunction with local computer supporters.

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.

EIS 100

Emergency access (i.e. an employee is incapacitated and another employee must enter the system to continue his job function) to electronic information shall be handled by the EIS during business hours and the Enterprise Information Security Analyst on call after business hours. 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.

Chapter 3 Processing Information and Documents

Subunit 1 Networks

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.

See CM 42 http://www.lsuhsc.edu/no/administration/cm/cm-42.htm

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.

EIS 100

Those responsible for managing the LSUHSC-NO network and preserving its integrity shall do so in accordance with the Office of Computer Services standards and job descriptions.

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.

EIS 100

All servers and workstations shall be configured according to LSUHSC-NO Enterprise Information Security standards (see Appendix) in order to safeguard LSUHSC-NO information system hardware, operation and application software, networks, and communication systems against both physical attack and unauthorized network intrusion.

All servers and workstations shall run anti-virus software (including spyware detection) while connected to LSUHSC-NO network infrastructure. In the event that the system will not operate properly with the anti-virus software, appropriate information security safeguards shall be instituted.

Subunit 2 System Operations and Administration

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.

ECS Hiring Policies

The Office of Enterprise Computer Services (ECS) shall appoint systems administrators who demonstrate the qualifications established by the department to manage the information technology systems and oversee the day to day security of these systems. Only qualified staff or third party technicians should repair information system hardware faults. System administrators must meet stringent qualifications for hire assuring that IT analysts are capable of handling analytic processes. HCSD IT personnel are hired through ECS.

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.

Covered by BAA's

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.

EIS 100

C.1 External Affiliates
External Affiliates are users who require access to LSUHSC-NO computer resources, but are neither LSUHSC-NO employees nor LSUHSC-NO students. Computer access for External Affiliates must be authorized by and coordinated through an affiliate sponsor for each different external affiliation.
C.1.1 External Affiliate Computer Accounts Computer access for External Affiliates is suitable only so long as the access is of benefit to the University. Once an affiliate separates from the
University, computer access must be revoked immediately.
C.1.2 External Affiliate Procedures

The Enterprise Information Security group shall maintain procedures for creating, modifying, and deleting access for external affiliations.

C.1.3 New External Affiliations

Computer Accounts for non LSUHSC-NO employees or students will be granted once their affiliation has been approved by LSUHSC-NO administration. New external affiliates shall be stored inside CRS and Enterprise Information Security procedures must be followed when creating these affiliations.

C.1.4 Deleting Access for External Affiliates

Accounts for External Affiliates shall be deleted according to the termination date set in the External User record when terminations are processed normally. External User, External Agency, and External Agency Department records shall never be deleted from CRS, even if the department or affiliation is no longer active.

C.1.5 External Affiliate Records Maintenance

Although the External Affiliate Sponsors are primarily responsible for informing Information Security of changes in the status of an affiliate's relationship to the University, Enterprise Information Security shall performs its own records maintenance to ensure that only people with active relationships with the University have computer access.

C.1.6 Requesting a New External Affiliation

Computer Accounts for non LSUHSC-NO employees or students will be granted once the affiliation has been approved by LSUHSC-NO administration. To establish an affiliation sponsorship, the head or chairman of the sponsoring department must submit the following:

a) A brief description of the relationship of the affiliation to LSUHSC-NO and how computer access will be of benefit to the University.

b) A description of the type of computer access required, e.g. email, SMS, PeopleSoft, etc.

c) An approximation of the number of individuals for who access will be required.

d) The name of the LSUHSC-NO employee(s) from the sponsoring department who will be the affiliation sponsor. The sponsor is responsible for coordinating with LSUHSC-NO Enterprise Information Security on all matters relating to the affiliation.

e) Acknowledgement that computer access for affiliates is suitable only so long as the access is of benefit to the University. Once an affiliate separates from the University, access must be removed immediately.

f) Acknowledgment that the sponsor assumes responsibility to immediately notify Information Security of changes in status with the University of any user under this affiliation.

g) Acknowledgment that the sponsor assumes responsibility to promptly notify Information Security whenever an affiliate's relationship with the University has terminated. The sponsor assumes responsibility for all activity associated with the accounts of terminated affiliates until such time that Information Security is notified to delete the account.

h) Acknowledgement that the sponsor is required to verify quarterly the status of each individual affiliate by indicating on spreadsheets provided by Information Security whether or not each person is still actively affiliated with the University.

i) Acknowledgment that Information Security must be notified 30 days prior to the account expiration date if an account is to be extended without any interruption in the user's access.

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.

HCSD shall implement the appropriate procedures within the Disaster Recovery Plan (DRP) 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.

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.

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

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.

Faculty, staff, students, and external users shall abide by CM-42 http://www.lsuhsc.edu/no/administration/cm/cm-42.htm which provides guidelines to ensure information, software, and media downloaded from the Internet does not jeopardize the operations, reputation, or security of the LSUHSC-NO and HCSD network.

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.

EIS 100

All email and/or any other form of digital communication generated by LSUHSC-NO information systems that contain 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 LSUHSC-NO information infrastructure without taking precautions to ensure the confidentiality and integrity of the information.

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.

EIS 100

All LSUHSC-NO and HCSD workstations shall have anti-virus software that scans emails and attachments. All inbound and outbound external and internal email shall be scanned for viruses on the email servers. The Office of Computer Services may also implement any procedures it feels necessary to ensure that malicious code is not delivered to or executed on LSUHSC-NO information systems by receiving email and/or any other form of digital communication.

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.

Procedure

Protected and/or restricted information should not be sent via email until LSUHSC-NO has developed and implemented procedures that ensure that emails and/or any other form of digital communication that contains protected or restricted information, including attachments, are correctly addressed and only being sent to appropriate persons. This procedure when developed 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.

Protected and/or restricted information can be sent electronically via Secure FTP, encrypted data on PCD's, or by giving protected access to a data drive.

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.

EIS 100

LSUHSC-NO and HCSD websites that contain protected or restricted information should be protected from unauthorized intrusion using website security standards. Only personnel who demonstrate the qualifications established by the Office of Computer Services should modify the campus website, especially if it contains protected information. These modifications shall be documented for audit purposes.

Subunit 4—Data Management

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.

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.

Subunit 5—Backup, Recovery, and Archiving

Policy Statement 3.5.1 —Transferring and Exchanging Data

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.

Chapter 4—Purchasing and Maintaining Commercial Software

Subunit 1—Purchasing and Installing Software

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.

Subunit 2—Software Maintenance and Upgrade

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.

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.

Procedure

The Disposition Phase represents the end of the systems life cycle. It provides for the systematic termination of a system to ensure that vital information is preserved for potential future access and/or reactivation. The system, when placed in the Disposition Phase, has been declared surplus and/or obsolete, and is scheduled to be shut down. The emphasis of this phase is to ensure that the system (e.g. software, data, procedures, and documentation) is packaged and archived in an orderly fashion, enabling the system to be reinstalled later, if desired. System records are retained in accordance with federal, state, university policies regarding retention of electronic records. (10 years) See Disposition Plan in Appendix D.

Chapter 5—Developing and Maintaining Custom Software

Subunit 1—Controlling Software Code

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.

EIS procedure

All operational program libraries for critical applications developed by LSUHSC-NO or HCSD shall reside on enterprise servers. Access to operational program libraries shall be controlled by the Enterprise Information Security group and will be provided on an as needed basis.

Policy Statement 5.1.2—Managing Program Source Libraries

LSU System campus shall implement a procedure in which only authorized staff may access program source libraries.

EIS procedure

All program source libraries for critical applications developed by LSUHSC-NO or HCSD shall reside on enterprise servers. Access to program source libraries shall be controlled by the Enterprise Information Security group and will be provided on an as needed basis.

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.

Subunit 2—Software Development

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.

EIS Procedure

Software developed by LSUHSC-NO or HCSD for systems identified as critical to campus operations must always follow a formal managed development process defined by the Office of Enterprise Computer Services. This process shall be appropriate for the size and scope of the system. All applications shall adhere to the Application Security Standards (see Appendix).

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.

Procedure

HCSD shall adhere to the security procedures mandated by LSUHSC-NO Enterprise Information Security (EIS) that provide for the controls for the security of protected or restricted data when used in the testing of new systems or system changes.

Subunit 3—Testing and Training Environments

Policy Statement 5.3.1—The Use of Protected Data for Training

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.

EIS Procedure

The use of protected or restricted data in the testing of new systems or system changes shall be adequately controlled. Access to operational test environments for critical applications shall be controlled by the Enterprise Information Security group and will be provided on an as needed basis.

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.

Procedure

All HCSD IT Directors will work with the application vendors, HR, Staff Development, and the developers of new applications to implement training plans for each new application prior to the application being put into production.

Chapter 6 Complying with Legal and Policy Requirements

Subunit 1 Complying with Legal Obligations

Policy Statement 6.1.1 Awareness of Legal Obligations

All LSU System campuses shall develop and implement procedures to inform employees of their legal responsibilities in relation to the use of computer based information and data.

HIPPA Security Training ROI and CM 42
http://www.lsuhsc.edu/no/administration/cm/cm-42.htm

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.

CM 42 http://www.lsuhsc.edu/no/administration/cm/cm-42.htm

Policy Statement 6.1.3 Computer Misuse: Legal Safeguards

Each LSU System campus shall implement a procedure by which employees are informed of changes in computer misuse federal or state law, as well as campus policy, as it directly impacts their job duties.

CM 42 http://www.lsuhsc.edu/no/administration/cm/cm-42.htm

Chapter 7 Business Continuity Planning

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

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.

Covered by DRP/BCP
Each LSUHSC-NO and HCSD campus shall follow procedures within the LSUHSC-NO IT Disaster Recovery Plan to ensure the continuation of key information services in the event that these services are disrupted. The LSUHSC-NO DRP shall be reviewed no less frequently than every three years and shall be revised if necessary to ensure new systems are integrated into the recovery procedures.

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.

Covered by DRP/BCP

Each LSUHSC-NO and HCSD campus shall conduct a formal risk assessment in order to determine any additional requirements for the LSUHSC-NO and HCSD Disaster Recovery Plan (DRP). Each LSUHSC-NO and HCSD campus shall review its risk assessment after each emergency and at least every three years.

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.

Covered by DRP/BCP

Each LSUHSC-NO and HCSD campus shall test the BCP/DRP at least annually and follow the appropriate procedures regarding testing. Results of testing shall be submitted to the LSU System Office of Executive Vice President. The BCP/DRP shall be produced in the appropriate format to guarantee its availability during an emergency.

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.

Chapter 8—Addressing Personnel Issues Relating to Security

Subunit 1 Contractual Documentation

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.

Procedure

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.

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

Covered by HIPAA IT Security training in ROI; see the EIS Computer account application at https://intranet.lsuhsc.edu/Forms/NO/Computer%20Account%20Application%20Form.pdf; and see CM42 at http://www.lsuhsc.edu/no/administration/cm/cm-42.htm.

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.

Policy Statement 8.1.3 External Suppliers/Other Vendor 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.

Procedure

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.

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.

The BAA can be found on page 29 of http://www.lsuhsc.edu/hcsd/policies/Public/Attachments/PM-36.pdf

Subunit 2—Personnel Information Security Responsibilities

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.

Covered by HIPAA IT Security training in ROI; see the EIS Computer account application at https://intranet.lsuhsc.edu/Forms/NO/Computer%20Account%20Application%20Form.pdf; and see CM42 at http://www.lsuhsc.edu/no/administration/cm/cm-42.htm.

Subunit 3—Employment Termination

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.

Procedure

The IT Director at each site will contact LSUHSC-NO EIS to immediately disable the account of any employee that represents a risk to the security of LSU System campus information. For all non-hostile terminations LSUHSC-NO EIS performs a nightly job that revokes access for all terminated employees.

Daily Maintenance of ID's by EIS:
The Enterprise Information Security group generates reports to determine terminations and transfers of users with access to computer resources. The transfer report compares selected information obtained from the User ID database and compares it against information that is reflected in the personnel databases to determine changes in position (i.e. a change in title, department, etc.). The termination report generates a list of faculty, staff, students, and external users in the personnel database that have permanently separated from the University.

In the event of a departmental change, EIS will terminate access to any administrative applications no longer needed in the user's new role. The appropriate authority will be notified by EIS to verify any access changes that are required due to the departmental change.

In the event of any termination, EIS will access the user's security information in the Computer Resource System (CRS, in-house developed program that uses a Sybase database to query access granted for any computer user of LSUHSC) and identify the computer access to remove. Once all access that a terminated user was granted has been identified in CRS, EIS will remove the Log-on ID/record from each individual system.

After the Security Group has completed removing access from the central systems (including archiving any datasets that the terminated user may have had stored on the mainframe), the computer support group for the user is notified by EIS to handle issues on the user end such as removing email access, home shares, etc.

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.

See local HR Policies.

Chapter 9 Training and Staff Awareness

Subunit 1 Awareness

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.

Covered by the EIS Computer account application at https://intranet.lsuhsc.edu/Forms/NO/Computer%20Account%20Application%20Form.pdf; and see CM42 at http://www.lsuhsc.edu/no/administration/cm/cm-42.htm
Orientation covers the HIPAA IT Security training in ROI.

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.

Procedure

Proposed changes or amendments to policies will be presented to the HCSD Compliance Committee for approval.

Updated policies will be distributed to HCSD Office personnel and to the hospitals for implementation.

The test portion of the HIPAA training will include a statement that the employee/resident understands that the information provided is a general overview, and communicates the expectation that the HCSD policies are to be reviewed in their entirety. The electronic record of this training will suffice as proof that this information was provided to the employee/resident.

The HCSD Director of Compliance will develop a mechanism in which this information is included in annual orientation and updates are communicated effectively throughout the organization.

In all of the training, it will be emphasized that the Compliance Officer/ Privacy Officer or Security Officer must be notified if these policies are not followed At that point, it will be determined if the employee/resident requires more in-depth education and training, or if the matter needs to be referred to Human Resources for disciplinary action.

Subunit 2 Training

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.

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.

Covered by ROI HIPAA IT Security Training

Standard HCSD general Compliance and HIPAA Privacy training modules and HCSD Information Security training modules have been developed to be presented to employees within the HCSD office and the hospitals by Compliance at General Orientation, Contracted Employee Orientation, and Resident Orientation. The information presented is an overview of the intent of each section, with the stated expectation that the employee/resident is to review the detailed HCSD policies. In cases in which the employee/resident does not have computer access, actual hard copies of the policies will be provided in the package. These methods will have an attestation that the employee/resident received the material. THESE MODULES WILL BE STANDARD FOR THE HCSD OFFICE AND ALL FACILITIES.

Chapter 10 Physical Security

Subunit 1 Campus Security

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.

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

Subunit 1 Reporting Information Security Incidents

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.

Procedure

All LSUHSC-NO and HCSD campuses shall adhere to the LSUHSC-NO Enterprise Information Security (EIS) and HCSD Incident Response Procedure above (See Policy Statement 1.6.2) and shall adhere to the Workstation and Server Standards in the Appendix and the Network Standards in the Appendix to help 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.

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.

Procedure

All LSUHSC-NO and HCSD campuses shall adhere to the LSUHSC-NO Enterprise Information Security (EIS) and HCSD Incident Response Procedure above (See Policy Statement 1.6.2). 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.

Subunit 2 Investigating Information Security Incidents

Policy Statement 11.2.1 Investigating the Cause and Impact of Information Security Incidents

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.

Procedure

All LSUHSC-NO and HCSD campuses shall adhere to the LSUHSC-NO Enterprise Information Security (EIS) and HCSD Incident Response Procedure above (See Policy Statement 1.6.2). 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 recurrence of similar incidents.

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.

Procedure

All LSUHSC-NO and HCSD campuses shall adhere to the LSUHSC-NO Enterprise Information Security (EIS) and HCSD Incident Response Procedure above (See Policy Statement 1.6.2). 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.

Chapter 12 Classifying Information and Data

Subunit 1 Setting Classification Standards

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.

Procedure

HCSD IT shall document mission and business critical applications that they are responsible for and update this documentation on an annual basis in a Risk/Critical Inventory Assessment.

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.

See Appendix for sample risk assessment inventory, instructions, and classification.

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.

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.

APPENDIX A

WORKSTATION AND SERVER STANDARDS

The purpose of these standards is to provide guidelines for best security practices when installing new workstations and servers (or reconfiguring older workstations and servers) on the LSUHSC-NO network. It is not the purpose of this document to provide the information necessary to correctly administer a workstation or server. It is assumed that the computer supporters responsible for implementing these standards are knowledgeable of the operating system they have chosen, the hardware on which it runs, and any applications they intend to install.

A.1 Workstation Standards

No workstation should be connected to the LSUHSC-NO network until the following items have been accomplished:

1. All security patches for the OS and any applications have been acquired using a local connection that does not require an IP address (e.g. USB hard drive, zip drive, CD, etc.)
2. All documentation for the workstation should be properly stored in a secure location.
3. The OS has been properly installed and configured and all relevant security patches for both the OS and any applications have been applied.
4. All unnecessary services have been disabled (e.g. HTTP, Telnet, FTP, SMTP, DNS, etc.). Only those services which are necessary for maintenance or to accomplish the task assigned to a workstation should be enabled. In practice this will mean disabling many services which are enabled by default. The specifics of any particular workstation are left to the computer supporter to determine.
5. All services that are installed on the workstation have been patched and secured properly before being enabled. Consult the vendor's documentation for proper security procedures for the application in question.
6. No workstations are allowed to run DNS, DHCP, NIS+, or a Windows Domain Controller under any circumstances.
7. A viable plan has been designed to maintain the workstation properly. This plan shall include consistent regular patching of the OS and all applications.
8. All passwords are in accordance with LSUHSC-NO password policy and Louisiana Office of Information Technology standards.
9. ALL default passwords must be changed immediately. Passwords should not be written down anywhere, so consider keeping an encrypted list of passwords on a separate, secure machine.
10. Access to administrator passwords should be limited to the smallest number of people necessary to properly maintain the workstation and allow access to in case of emergencies.
11. "Owners" should not use an account that has administrative access to the workstation for routine work. A separate account should be used for administrative access (such as "root" or "Administrator") and the owner should use utilities such as "su", "sudo", or "runas" or login as the administrator when administrative access is required and logout when the work is completed.
12. No workstation should be connected to the LSUHSC-NO network unless it has virus and spyware protection in place and it has been properly configured and updated.

13. Every workstation should use a dynamically assigned IP address. If the workstation requires a static IP address, the computer supporter should consult with LSUHSC-NO OCS to establish the requirements.
14. If the OS provides a stateful firewall (e.g. Windows Firewall, ipchains, iptables, ipfw, etc.), it should be enabled and only outgoing traffic should be allowed.
15. All workstations should have access logging enabled.
16. The use of encryption (e.g. VPN) is required for remote access to workstations. Only those in the administrator group should be allowed to remotely access a workstation.

A.2 Server Standards

No server should be connected to the LSUHSC-NO network until the following items have been accomplished:

All security patches for the OS and any applications have been acquired using a local connection that does not require an IP address (e.g. USB hard drive, zip drive, CD, etc.)

All documentation for the server should be properly stored in a secure location.

The OS has been properly installed and configured and all relevant security patches for both the OS and any applications have been applied.

All network application services not essential to the prime function of the server have been disabled – HTTP, Telnet, FTP, SMTP, DNS, etc. No services should be enabled unless they have been patched to current levels and are necessary to accomplish the task assigned to a server.

No servers are allowed to run LDAP, DNS, DHCP, NIS+, or a Windows Domain Controller without prior coordination with LSUHSC-NO OCS.

A secure location has been identified for the server. Servers should never be physically accessible to anyone but the “owners”. They should be in designated server rooms or in locked offices which can only be accessed by the “owners”.

A viable plan has been designed to maintain the server properly. This plan shall include consistent regular patching of the OS and all applications.

All passwords must be in accordance with LSUHSC-NO password policy and Louisiana Office of Information Technology standards.

ALL default passwords must be changed immediately. Passwords should not be written down anywhere, so consider keeping an encrypted list of passwords on a separate, secure machine.

Access to administrator passwords should be limited to the smallest number of people necessary to properly maintain the workstation and allow access to in case of emergencies.

Server administrators should supply accurate contact information to LSUHSC-NO OCS for emergencies such as power outages and server break-ins. This information should also include a general description of the server, its purpose, and any special requirements or configuration.

No server should be connected to the LSUHSC-NO network unless it has virus protection in place or it has been determined that it is not necessary for that server.

Every server should be plugged in to an Uninterruptible Power Supply (UPS).

Every server should have an appropriate name and static IP address.

No servers should be connected to the LSUHSC-NO network unless qualified personnel are in place to administer the server.

If the OS provides a stateful firewall (e.g. Windows Firewall, ipchains, iptables, ipfw, etc.), it should be enabled and only those ports necessary to allow the server to function should be open.

Remote logging (syslogging) should be enabled on all enterprise application servers.

If it is determined to be necessary, remote access to servers should be highly restricted.
The use of encryption (e.g. VPN, SSH) is required for remote access to servers. Only those authorized as administrators on a server should be allowed access the server remotely.
Owners of vendor controlled equipment should consult with LSUHSC-NO Enterprise Information Security regarding special needs before connecting to the network. Vendor controlled equipment includes special instrumentation (such as mass spectrometers, electron microscopes, specialized medical equipment, etc.), application software that requires a certain Service Pack or patch level and cannot be patches to current levels, FDA approved equipment which cannot be altered in any way without losing FDA approval and similar types of equipment where the vendor or some other non-LSUHSC entity controls what patching may be done to a server.
Consideration should be given to both internal and external threats to the server, especially for equipment that falls under the guidelines of HIPAA.
All information technology equipment used for research funded by grants must be in compliance with Federal, State, and LSUHSC-NO guidelines.
LSUHSC-NO password policy should be maintained for any accounts on the vendor's server.
Best practices for both the operating system and the applications on the server should be followed as much as is practical, within the constraints the vendor has defined.

Below are links to suggested reading:
NIST National Vulnerability Database
[http://nvd.nist.gov/]
NIST Computer Security Resource Center
[http://csrc.nist.gov/]
Microsoft TechNet Security Center
[http://www.microsoft.com/technet/security/]
CERT Coordination Center
[http://www.cert.org/]
EDUCAUSE Computer and Network Security Task Force
[http://www.educause.edu/security]
National Security Agency – System and Network Attack Center
[http://www.nsa.gov/snac/]
The Center for Internet Security
[http://www.cisecurity.org/]
SANS Information Security Resources
[http://www.sans.org/resources/]
SANS Top 20 Vulnerabilities
[http://www.sans.org/top20/]

APPENDIX B
NETWORK WIRING STANDARDS

See Attachment

APPENDIX C

LSUHSC-NO EIS 100 - Application Security Requirements

1. Windows Active Directory equivalent security compatibility to identify and authenticate single user at both system and application level
2. If software uses Active Directory, it should not require a schema change.
3. If software uses Active Directory and requires domain controller configuration, it should allow for multiple server entries for failover.
4. User roles/classifications should be configurable and granular enough to meet user specifications.
5. Changes to roles/classification should automatically affect all users that are assigned to the role/classification.
6. Software should have the ability to add new roles/classifications.
7. Software should allow for the separation of duties between System and Security Administrators (System Administrator should not have access to security menu options).
8. Users should not have access to the data; software runs under an “application account.”
9. Software should have the ability to implement row security by hospital and/or department.
10. Software should allow userids/logonids to be reused and not interfere with audit logs.
11. Software should audit changes to data, changes to security, logon/logoff activity.
12. Software should allow the resetting of passwords service/application accounts (no hard-coded passwords) should they be compromised.
13. Shall allow single user and/or group limitation or denial at various levels within the application. Including read-only provision.
14. Automatic logout after user defined time period (user customizable).
15. Shall provide audit trails for date, time and user attempts.
16. Shall provide ability to deny access for failure to correctly enter login id or password for attempts not in specifically single user approved (start/stop) date ranges within the ED application (understand that may be continued legitimate enterprise user but not authorized in ED system).
17. Ability for remote access and method.
18. User roles or classifications are definable and can be limited at individual and group level by the system administrator.

APPENDIX D

SAMPLE DISPOSITION PLAN
US Department of Justice

INTRODUCTION

The Disposition Plan is the most significant deliverable in the disposition of the information system, and the plan will vary according to system and Department requirements. The objectives of the plan are to end the operation or the system in a planned, orderly manner and to ensure that system components and data are properly archived or incorporated into other systems. At the end of this task, the system will no longer exist as an independent entity. The completion of the systems life cycle is carefully planned and documented to avoid disruption of the organizations using the system or the operation of other systems that will use the data and/or software of the present system.

The Disposition Plan needs to be an extension of the Records Management function. Records Management— what is kept, what is a legal "record," retention period, etc.-- is a topic beyond the scope of this SDLC. The software, hardware, and data of the current system are disposed of in accordance with organization needs and pertinent laws and regulations. Software or data of the system may be transferred to other existing systems, migrated to an entirely new system, or archived for future use. Hardware is made available for future use, added to surplus, or discarded.

In conducting the disposition task, the following items should be considered:

- All known users should be informed of the decision to terminate operation of the system before the actual termination date.

- Although the current system may be terminated, in many cases the data will continue to be used through other systems. The specific processing logic used to transfer the data to another system is developed as part of the data conversion planning for that system.

- In some instances, software may be transferred to a replacement system. For example, a component of the current system may become a component of the replacement system without significant rewriting of programs.

- Effective reactivation of the system in the future will depend heavily on having complete documentation. It is generally advisable to archive all documentation, including the life-ycle products generated during the earliest tasks of the life cycle as well as the documentation for users and for operation and maintenance personnel.

The Disposition Plan addresses how the various components of the system are handled at the completion of operations, including software, data, hardware, communications, and documentation. The plan also notes any future access to the system. The plan is lead/performed

by the Project Manager; supported by the records management staff, the project team, and the functional staff; and reviewed by the QA manager. Other tasks include the following:

- Notify all known users of the system of the planned date after which the system will no longer be available. Work with the FOIA/PA representative process any Federal Register regarding system of records notification.

- Copy data to be archived onto permanent storage media, and store media in a location designated by the Disposition Plan. Work with the project management team for other systems to effect a smooth transfer of data from the current system to these systems.

- Copy software onto permanent storage media, and store media in location designated in Disposition Plan. (Software to be stored may include communications and systems software as well as application software.) Work with the project team for other systems to ensure effective migration of the current system software to be used by these systems.

- Store other life-cycle products, including system documentation, in archive locations designated by the Disposition Plan.

- Dispose of equipment used exclusively by this system in accordance with the Disposition Plan (refer to excess procedures).

- Complete and update the Disposition Plan to reflect actual disposition of data, software, and hardware.

- Plan for the shutdown of the project, including the reassignment of project staff, the storage of project records, and the release of project facilities

PARTS OF THE PLAN

1.0 INTRODUCTION

This section provides a brief description of introductory material.

1.1 Purpose and Scope

This section describes the purpose and scope of the Disposition Plan. Reference the information system name and provide identifying information about the system undergoing disposition.

1.2 Points of Contact

This section identifies the System Proponent. Provide the name of the responsible organization and staff (and alternates, if appropriate) who serve as points of contact for the system disposition. Include telephone numbers of key staff and organizations.

1.3 Project References

This section provides a bibliography of key project references and deliverables that have been produced before this point in the project development. These documents may have been produced in a previous development life cycle that resulted in the initial version of the system now undergoing disposition or may have been produced in subsequent enhancement efforts as appropriate.

1.4 Glossary

This section contains a glossary of all terms and abbreviations used in the plan. If it is several pages in length, it may be placed in an appendix.

2.0 SYSTEM DISPOSITION

2.1 Notifications

This section describes the plan for notifying known users of the system being shut down, and other affected parties, such as those responsible for other, interfacing systems, and operations staff members involved in running the system.

2.2 Data Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the data files and related documentation in the system being shut down.

2.3 Software Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the software library files and related documentation in the system being shut down.

2.4 System Documentation Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the hardcopy and softcopy systems and user documentation for the system being shut down.

2.5 Equipment Disposition

This section describes the plan for archiving, deleting, or transferring to other systems the hardware and other equipment used by the system being shut down.

3.0 PROJECT CLOSEDOWN

3.1 Project Staff

This section describes the plan for notifying project team members of the shutdown of the system, and the transfer of these team members to other projects.

3.2 Project Records

This section describes the plan for archiving, deleting, or transferring to other projects the records of project activity for the project that has been maintaining the system being shut down.

3.3 Facilities

This section describes the plan for transferring or disposing of facilities used by the project staff for the system being shut down.

DISPOSITION PLAN OUTLINE

Cover Page
Table of Contents
1.0 Introduction
- 1.1 Purpose and Scope
- 1.2 Points of Contact
- 1.3 Project References
- 1.4 Glossary

2.0 System Disposition
- 2.1 Notifications
- 2.2 Data Disposition
- 2.3 Software Disposition
- 2.4 System documentation Disposition
- 2.5 Equipment Disposition

3.0 Project Closedown
- 3.1 Project Staff
- 3.2 Project Records
- 3.3 Facilities

APPENDIX E
RESOURCE SURVEY SAMPLES
Resource Inventory

Site:

					Contains PHI (Y/N)	Contains Financial Information (Y/N)	Owner		Value		Security Classification			Loss Potential										
														Denial of Service			Corruption of Data			Disclosure			Destruction of Data		
	Identifier	Application Area	Application Name	Vendor			Department	Individual	Dollars	Determination	Confidentiality	Integrity	Availability	Time	Money	Quality of Service	Time	Money	Quality of Service	Time	Money	Quality of Service	Time	Money	Quality of Service

Application Protected/Restricted Information Inventory

Application Area
Accounting
Admitting
Appointment/Resrouce Sch
Biomed
Call Accounting
Cardiology
Central Supply
Chart Reservation/Tracking
Coding
Contract Services
Dietary
Education
Emergency Department
Employee Equal Opportunity
Employee Health
Environmental Management
Equipment Maintenance
Facilities Management
Finance
Grants Management
HIV Clinic
Home Health
Human Resources
Immunization
Infection Control
Information Systems
Inventory Control
JCAHO Compliance
Lab
LSUHSC-MD Billing
Medical Records
Medical Staff
Medical Staff
Nursing
Nursing In-Service
Patient Accounting
Payroll
Performance Improvement
Pharmacy
Property Control
Psychiatric Services
Purchasing
Radiation Onocolgy
Radiology
Student Administration
Respiratory
Surgery Scheduling System
Time/Attendence

PHI
Names;
Address: street address, city, county, precinct, ZIP code, and their equivalent geocodes. Exc
The geographic unit formed by combining all ZIP codes with the same three initial digits c
The initial three digits of a ZIP code for all such geographic units containing 20,000 or few
Note:
The 17 currently restricted 3-digit ZIP codes to be replaced with '000' include: 036, 059, 063,
All elements of dates (except year) for dates directly related to an individual including:
Birth date
Admission date
Discharge date
Date of death
And all ages over 89 and all elements of dates (including year) indicative of such age. Such
Telephone numbers;
Fax numbers;
Electronic mail addresses;
Social security numbers;
Medical record numbers; (including prescription numbers and clinical trial numbers)
Health plan beneficiary numbers;
Account numbers;
Certificate/license numbers;
Vehicle identifiers and serial numbers including license plate numbers;
Device identifiers and serial numbers;
Web Universal Resource Locators (URLs);
Internet Protocol (IP) address numbers;
Biometric identifiers, including finger and voice prints;
Full face photographic images and any comparable images; and
Any other unique identifying number, characteristic, or code; except a code used for re-iden
The facility does not have actual knowledge that the information could be used alone or in c

Instructions For Filling Out Resource Inventory

Instructions for filling out Resource Inventory

General	Please list every information system in use on your campus on this spreadsheet. Please include any systems that are completely supported either by a department or by a vendor. The key critieria is that the system is used by faculty staff or students.
Site	Three letter site code
Indentifier	Reserved
Application Area	Business function served by the application.(See "Application Area" column on "Lists" worksheet)
Application Name	Name of application
Vendor	Name of vendor
Contains PHI(Y/N)	Does the system store protected health information?(Medical or billing information plus any of the identifiers listed in the "PHI" column on the "Lists" worksheet)
Contains Financial Information(Y/N)	Does the system store financial records
Owner	The one responsible for collecting and maintaining the data on the system.
Department	The department responsible for collecting and maintaining the data in this system
Individual	The person with the primary responsibility for collecting and maintaining the data on this system who provides the rankings.
Value	The monetary value of the system broken down in two parts
Cost	The actual dollar value of the data.
Determination	How the dollar amount was arrived at (creation, re-creation, unavailability, disclosure)
Security Classification	Classification of the information based on its importance to the organization in three areas
Confidentiality	Rate the confidentiality of the data on this system based on the following scale: 0 - Public data - Information available to anyone. Examples: Promotional materials, de-identified data. 1 - Restricted use - Data with some indirect identifiers such as census tract or zip code that is used for a specific purpose such as service benchmarking.

	2 - Internal only - Data used internally by the organization of its own operations. Examples include budgets, insurance ratings, etc.
	3 - Confidential - Data whose disclosure would result in a violation of confidence and expose the organization to civil and criminal penalties. Examples of this kind of data are patient health information, employee payroll data.
	4 - Highly Sensitive - Data that requires extraodinary steps to insure its confidentiality due to its sensitive nature. Examples include HIV status, mental health progress notes.
Integrity	0 - Accuracy of the data is not important.
	1 - Data is very dynamic and is updated frequently. Statistical aggregates are more useful than individual data points.
	2 - Accuracy is important. When errors are found corrections must be made but no deadline is imposed.
	3 - Accuracy is important. When errors are found, they must be corrected within a few days.
	4 - Accuracy of data is of paramount importance. Any errors must be corrected immediately and users notified. Data is kept for lengthy periods and is used in an historical fashion.
Availability	0 - Business functions that can be interrupted and where the availability is not essential. To the user work stops and an uncontrolled shutdown occurs. Data may be lost or corrupted.
	1 - Business functions can be interrupted as long as the availability of the data is insured. To the user, work stops and an uncontrolled shutdown occurs. A backup copy of the data is available on a redundant disk or tape and a log-based or journal file s
	2 - Business functions that allow minimally interrupted computing services, either during essential time periods, or during most hours of the day and most days of the week throughout the year. This means that the user will be interrrupted but can quickly
	3 - Business functions that require uninterrupted computing services, either during essential time periods, or during most hours of the day and most days of the week throughout the year. This means that the user stays on-line. However the current transact

	4 - Business functions that demand continuous computing services and where any failure is transparent to the user. This means no interruptions of work; no transactions lost; no degradation in performance; and continuous 24x7 operation.
Loss Potential	An analysis of the losses expected to occur in time, money and reduction of quality of service for each of the types of losses. Time and money can be presented two different ways. If, for example, you know that a restore of data for a particular system re
	0 - No impact on delivery of services, work performed by users, or delivery or quality of patient care.
	1 - Small but measurable impact on delivery of services, work performed by users, or delivery or quality of patient care.. Not big enough for users to notice
	2 - Users and/or patients may notice the impact on services but the impact is easily mitigated. Delivery of services is inconvenient for staff but quality of care is not affected.
	3 - Large impact that involving considerable inconvenience to users and /or patients, data not available to decision makers, patient care impacted, etc.
	4 - Services can not be performed. Risk to health and safety.
TYPES OF LOSSES	
Denial of Service:	Services provided by this system are not available due to equipment malfunction, hacker attack, virus infection, natural disaster, etc.
Corruption of Data:	Data on this system becomes unreliable due to malfunction, human error, etc.
Disclosure:	Information stored on this system is released to unauthorized persons or made public by human error, disgruntled employees, etc.
Destruction of Data:	Data is lost due to equipment malfunction, natural disaster, human error, or malicious acts, etc.

(goto top)