

**LSU HEALTH CARE SERVICES DIVISION
BATON ROUGE, LOUISIANA**

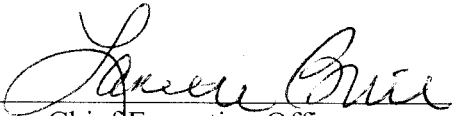
POLICY NUMBER: 7701-17

CATEGORY: Information Security

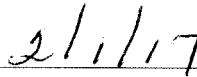
CONTENT: Information System and Data Security

EFFECTIVE DATE: Issued: April 26, 2005
Reviewed, Revised, Reissued: May 18, 2009
Reviewed: August 10, 2010
Reviewed: November 14, 2011
Reviewed, Revised: March 15, 2015
Reviewed, Revised: February 1, 2016
Reviewed: January 26, 2017

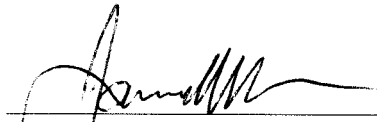
INQUIRIES TO: James "Mickey" Kees, CIO
LSU Health Care Services Division
P.O. Box 91308
Baton Rouge, LA 70821-1308
Telephone 225-922-0775 or 318-330-7594
Facsimile 225-922-1502



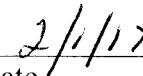
Deputy Chief Executive Officer
LSU Health Care Services Division



Date



Chief Information Officer
Chief Medical Information Officer
LSU Health Care Services Division



Date

Table of Contents

Introduction	3
Chapter 1 – Securing Systems, Hardware, Software and Peripherals	5
Chapter 2 – Controlling Access to Information and Systems	15
Chapter 3 – Processing Information and Documents	23
Chapter 4 – Purchasing and Maintaining Commercial Software	29
Chapter 5 – Developing and Maintaining Custom Software.....	30
Chapter 6 – Complying with Legal and Policy Requirements	31
Chapter 7 – Business Continuity Planning.....	32
Chapter 8 – Addressing Personnel Issues Relating to Security.....	33
Chapter 9 – Training and Staff Awareness.....	36
Chapter 10 – Physical Security.....	37
Chapter 11 – Protecting For, Detecting and Responding to Information Security Incidents.....	38
Chapter 12 – Classifying Information and Data.....	39
Appendix A – Workstation and Server Standards.....	41
Appendix B – Application Security Guidelines	44
Appendix C – Disposition Plan	46
Disposition Plan Checklist	48
Appendix D – Data Sanitization – Standards and Requirements.....	50
Appendix E – Portable Computing Device Release Form	59

Introduction

I. Purpose

The purpose of this policy document is to provide guidance to all LSU HCSD employees in meeting our organization's need to appropriately secure the systems and information critical to maintaining clinical and administrative operations. This policy and procedure guidance has as its basis the broader LSU System Information Security Plan (PM36), and the policies and procedures outlined in LSU HCSD 7521 (HIPAA Administrative, Technical and Physical Safeguards), LSU HCSD 4511 (Email) and LSU HCSD 4512 (Internet), LSUHNO CM 42 (Information Technology Infrastructure), LSUHNO EIS 100 (LSUHSC New Orleans Security Policy), and the regulations of the Louisiana Office of Information Technology.

II. Scope

This policy document sets the Information Security standard for all LSU HCSD facilities. This policy shall apply to each officer, director, employee, leased employee, student and agent of LSU HCSD. Comprehensive verbiage is not necessarily transferred from the policies outlined in the Purpose to this document. As such, all LSU HCSD personnel are required to be familiar with and maintain an understanding of this document, as well as each of the policies outlined in the Section I. Purpose, and any additional information security standards set by LSU HCSD or the regulatory agencies by which health care delivery organizations are required to comply.

While this Information Security policy uses as its basis LSU PM36, it seeks to extend LSU PM36 by interpreting its policy statements in the context of LSU HCSD's business operations. It also seeks to highlight, extend and/or amend other policies in an effort to comprehensively cover the broad scope of information security as it applies to a health care delivery organization within a state university system. Excerpts from a variety of policies, such as LSUHNO EIS 100, are contained within this document for the convenience of the reader. It is recommended the reader consult, as necessary, the original policy from which these excerpts have been taken.

Information Security and Data Security is specific to the operations of LSU HCSD, and is derived in part from PM-36 and EIS-100. As of the first quarter of 2015, PM-36 is being updated and revised. 7701 -15 includes exceptions noting processes that currently differ from PM-36. These exceptions will be reconciled once PM-36 is updated.

Note: Language taken directly from PM36 is represented in italics.

III. Definitions

A. Protected Information

Protected information includes but is 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. For the purposes of LSU HCSD, the definition of protected information is extended explicitly to be inclusive of "protected health information" as defined by HIPAA regulations.

B. Restricted Information

Restricted information includes but is not limited to ongoing investigations, pending litigation, psychology notes and disciplinary action. For the purposes of LSU HCSD, the definition of restricted information is extended explicitly to be inclusive of “protected health information” as defined by HIPAA regulations.

C. Facility

A facility for the purpose of this policy is defined as any LSU HCSD location where information and systems are used, maintained or stored. This includes LSU HCSD hospitals, LSU HCSD headquarters (HQ) and all physical locations related to the hospitals or headquarters.

D. Hospital

A hospital for the purpose of this policy is defined as any LSU HCSD hospital facility. This excludes the LSU HCSD HQ facility.

E. System Owner

A system owner is the director(s) and/or supervisor(s) of the functional area(s) for which a system is implemented and maintained to support the work activities of the personnel in those functional areas. For systems serving similar functional areas across multiple LSU HCSD facilities, the system owner shall be the LSU HCSD HQ director or supervisor to which facility directors/supervisors report.

IV. Implementation

This policy and any subsequent revisions to this policy shall become effective upon the approval date and signature of the Chief Executive Officer of LSU HCSD (or designee).

V. Consequences

Any employee, faculty, staff, student or agent of LSU HSCD found to be in violation of the provisions of the LSU HCSD Information Security Policy will be subject to appropriate disciplinary action, up to and including termination of employment/ enrollment.

VI. Policy and Procedure Statements

LSU HCSD Information Security Policy / Procedure statements are embedded within the retained outline of LSU PM36 (below). This has been done to provide consistent structure and ease with updating this document as changes might occur to LSU PM36.

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.

LSU HCSD Policy / Procedure

All LSU HCSD facilities shall adhere, in addition to the policy contained herein (7701), in whole or in part, as designated in LSU HSCD Policy / Procedure statement to each of the following Information Security standards:

1. LSU HCSD 7521 (HIPAA Administrative, Technical and Physical Safeguards)
2. LSU HCSD 4511 (Email) and 4512 (Internet)
3. The LSUHNO Enterprise Information Security (EIS) 100 Workstation and Server Standards and Application Security Guidelines (Appendix A and B)
4. LSUHNO CM 42 (Information Technology Infrastructure)
5. Any additional information security standards set at an LSU HCSD facility that are more restrictive than the above

All standards shall be reviewed on an annual basis with a review date.

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 approvals prior to purchase.

LSU HCSD Policy / Procedure

All proposed IT projects and systems, whether vendor based or in-house developed, shall be reviewed by the facility IT Director and/or IT Security Officer for adherence to LSU HCSD Information Security standards, and approved in writing, prior to purchase and prior to implementation. Any proposed IT project that requires LSUHNO or HCSD enterprise resources must be approved by the HCSD CIO. Failure to complete this review and approval may result in delay or discontinuance of a project.

To support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Enterprise Information Security(EIS), LSU HCSD has adopted the LSUHNO EIS workstation and server standards and application security guidelines. The facility IT Director and/or IT Security Officer will review and approve new information systems according to these guidelines and other applicable state or federal requirements (i.e. HIPAA), and LSU HCSD policies and procedures.

See Appendix A - Workstation and Server Standards

See Appendix B – Application Security Guidelines

Policy Statement 1.1.3 – Installation, Upgrade and Testing of Hardware, Systems, and Equipment

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

LSU HCSD Policy / Procedure

All information technology-related hardware, systems, software, upgrades and patches that are installed or implemented represent a change in system or information accessibility, availability or security. Information technology-related hardware, systems, software, upgrades and patches that are installed or implemented shall be fully and comprehensively tested when appropriate and testing capabilities are available, and authorized by management of the technical and operational areas to be affected by the change, prior to being converted to a “live” environment. All change actions shall be weighed against the potential outcome of not making the change, and the extent of planning and testing of the change shall be appropriate to the size and complexity of the installation, as defined by the directors of departments affected by the change and/or the system owner. This shall be done to ensure the security of the systems and information with minimal disruption of operations. The planning and testing shall include consideration of each of the following points:

1. Any significant system change that likely has or has the expected potential to affect a user group shall be planned with the knowledge and cooperation of that group. 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 system or its data.
2. The determination of “likely” or “expected” shall be examined in the most conservative way possible to minimize or eliminate the chance of service interruption, or compromise of data availability or integrity. Likely or expected should include any change that involves documented known faults, is provided untested by the vendor, is applied to a system that has local customizations that could not be tested by the vendor, or involves the need for extended downtime.
3. 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.
4. Any system that contains restricted or protected information shall be backed up with a restore point prior to implementing the change.
5. Critical software updates for known vulnerabilities may take precedence over a group’s productivity but shall not occur without the knowledge and cooperation of that group.
6. All significant system changes shall be documented with the details of the change and the date of occurrence.

Subunit 2 – IT Peripherals

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.

LSU HCSD Policy / Procedure

Senior Staff at each HCSD facility are responsible for designating the criticality of information systems supporting their area as (1) “high” to ongoing operations thus requiring 24/7 high availability, (2) “moderate” to ongoing operations but capable of tolerating service disruptions lasting no more than four [4] hours, or (3) “low” to ongoing operations and capable of tolerating service disruptions lasting more than four [4] hours. Directors are responsible for communicating this system availability requirement to their facility IT Director, and updating the IT Director whenever a status change in this availability requirement occurs.

Facility IT Directors are responsible for assuring the protection of all information systems designated as high, independent of their physical location at a local or central data center, with an uninterruptible power supply (UPS) and emergency power adequate to provide continuity of services. All information systems designated as high, or moderate must have power management protection adequate to provide an orderly shutdown to preserve data integrity in the event of a catastrophic or unavoidable disruption.

Facility IT Directors are responsible for maintaining an inventory of all information systems and hardware to include the criticality of those systems as “high, moderate or low”. Senior Staff in conjunction with the facility IT Director shall review and update the criticality of their information systems on an annual basis. Systems with a criticality of high or moderate must be documented in the local disaster recovery plan.

Uninterruptible power supplies shall be maintained and tested according to manufacture 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.

LSU HCSD Policy / Procedure

Each LSU HCSD facility shall review and update its inventory of systems requiring high availability on an annual basis. Systems with a criticality of high or moderate must be included in the facility Disaster Recovery Plan (DRP).

Policy Statement 1.2.3 – Using Fax Machines/Fax Modems

Protected or restricted information may be faxed when it is necessary and deemed a secure method of communication.

LSU HCSD Policy / Procedure

The sender of the protected or restricted information and the intended recipient shall agree to the fax as an appropriate method for transmittal prior to sending. Documents containing personal identifiers shall only be faxed with appropriate safeguards. Protected or restricted information shall not be sent to a fax machine in an unsecured area. Appropriate physical safeguards or an authorized person shall be present to safeguard the receipt of protected or restricted information during and after fax transmission. Senders and recipients are responsible for ensuring that faxes are picked up as timely as practicable. Directors are responsible for determining that fax machines in their operational areas are appropriately secure for the type of information transmitted to/from such equipment in support of business operations. Directors are responsible for their department's adherence to the Safeguarding Faxes policy.

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.

LSU HCSD Policy / Procedure

In the event that protected or restricted information cannot be sent via LSU Health System network, additional precautions (e.g. virtual private network, encryption of data) shall be employed to ensure against unauthorized interception and/or disclosure of protected information. Facility IT directors shall assist users in determining the best method to employ for the transfer of data outside of the LSU Health System network. Enterprise Network Support and Enterprise Information Security shall be consulted prior to installing any VPN, SFTP, or other secure file transfer application.

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.

LSU HCSD Policy / Procedure

Documents containing protected or restricted information shall only be printed with appropriate safeguards. Protected or restricted information shall not be sent to a printer in an unsecured area. Individuals that initiate the printing of documents are responsible for ensuring they are picked up as timely as practicable. Directors are responsible for determining that printers in their operational areas are appropriately secure for the type of information printed from such equipment in support of business operations. All users shall take precautions to ensure that they are choosing the correct printer when given a choice of printers in the application they are using.

Policy Statement 1.2.6 Securing Network Cabling

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

LSU HCSD Policy / Procedure

All LSU HCSD facility network cabling shall be appropriately physically secured to prevent unauthorized interception, tampering or damage. The identification of potential security compromises related to network cabling should be reported immediately by employees to their supervisor and/or the facility IT Director.

Subunit 3 – Removable Media

Policy Statement 1.3.1 – Using Removable Storage Media Including Diskettes and CDs

The removal of protected or restricted information from campus premises shall require specific authorization from the campus designated official.

LSU HCSD Policy / Procedure

The use of removable media to store or transport protected or restricted information is prohibited, without appropriate administrative approval. Protected or restricted information shall not be stored on removable media (including floppy disks, USB flash drives, CDs, DVDs, etc) unless such storage is absolutely necessary to support a defined business need. All protected or restricted information stored on removable media shall be kept in a secure physical environment on the campus of an LSU HCSD facility, unless removal from the premises is required to support a defined business need. All employees shall take appropriate measures to ensure that protected or restricted information is not disclosed to anyone other than to those individuals designated by management to receive or use such information. Physically taking protected or restricted information off campus, whether in digital or hardcopy form is to be avoided. The removal of protected or restricted information from LSU HCSD facility premises shall occur only in support of a defined business need and only with the documented approval (written or electronic) of the employee's director in accordance with the following points:

1. Appropriate administrative approval has been secured
2. All information is kept securely concealed and inaccessible to others by physical means and use of encryption
3. Only the employee has knowledge of or access to the information during transport while off campus
4. Only the minimum information necessary to accomplish the task is transported off campus
5. Removable media used for transport is "sanitized" or destroyed, not just erased, immediately upon completion of the assigned task (See 1.6.1)

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 with 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.

LSU HCSD Policy / Procedure

Third party access to LSU HCSD information or systems containing protected or restricted data shall be granted only after a contract is executed with the third party; the contract is accompanied by a signed Business Associate Agreement. In those situations where the need for third party access to LSU HCSD information or systems containing protected or restricted data is not accompanied by a contractual agreement (e.g. data sharing for the purpose of patient care continuity with community partner provider organizations), access to data shall be granted only after an information sharing agreement is in place and executed between LSU HCSD and the third party.

The LSU HCSD BAA standard template can be found at: <http://www.lsuhschools.org/docs/7510-15.pdf>

Also see Policy Statement 3.2.3 – Permitting Third Party Access.

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 data stored on that device is properly backed up, 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. Persons are responsible for its security at all times.

LSU HCSD Policy / Procedure

Only authorized personnel shall be permitted to take LSU HCSD laptops or other portable computing devices off the premises of their local facility, and are responsible for security of the device at all times. Directors are responsible for authorizing the possession and use of a portable computing device for their employees. The facility IT Director is responsible for documenting to whom a portable computing device is assigned and that the individual has signed the LSU HCSD Portable Computing Device Use Agreement (Appendix E).

The safety and security of portable computing devices is the responsibility of the authorized employee to whom the device is assigned. Portable computing devices shall be stored in a secure, locked location when not in use. Portable computing devices should not be out-of-sight of the employee when not secured. During travel off campus, portable computing devices 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, portable computing devices shall be stored with hotel security when the employee must leave the device at the hotel for an extended period of time. Loss of a portable computing device shall be reported immediately to the facility IT Security Officer and Privacy Officer. Additional reporting shall also be made to law enforcement, Legislative Auditor and local District Attorney in accordance with state law and LSU HCSD policy 2523.

Each LSU HCSD employee who is assigned a portable computing device shall be responsible for ensuring that the device is connected to the LSU Health System network at least once per week. This is necessary to insure the operating system, virus definitions, and applications are updated timely. The connection to the network can be accomplished either by bringing the device to a LSU HCSD location to connect it via a wired or wireless network, or via the LSU remote access VPN connection. If the employee assigned a portable computing device is unfamiliar with how to accomplish these responsibilities, he or she shall contact the facility IT Director for assistance.

The IT Director at each facility is responsible to maintain a listing of all portable computing devices assigned by the facility and who is in possession of the devices. The IT Director at each facility is also responsible to insure all portable computing devices are configured to receive operating system, virus definition, and application updates automatically when the device is connected to the LSU

Health System network. Any change in the possession of a portable computing device shall be reported immediately by the employee documented as having possession of the device and the employee taking possession of the device to the facility IT Director.

Policy Statement 1.4.3 – (Teleworking) or Working from Home or Other OffSite Location

LSU System campuses that allow teleworking or working from home shall establish procedures to ensure the confidentiality, integrity and availability of protected data accessed during any teleworking session.

LSU HCSD Policy / Procedure

LSU HCSD employees working from off-campus locations and using computer equipment issued by LSU HCSD for the purpose of supporting such work, shall abide by the same policies and procedures for accessing and maintaining protected or restricted information as when working on campus. When using an LSU HCSD issued computer or portable computing device from home or when traveling, the screen (monitor) should be placed so it will not be visible to non-authorized personnel. All teleworking sessions involving network connectivity to LSU Health systems or information shall require an encrypted connection (VPN or Citrix) to the LSU Health System Network to ensure against unauthorized interception and/or disclosure of information. Printing of PHI at remote location is prohibited.

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.

LSU HCSD Policy / Procedure

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, disposal.

LSU HCSD Policy / Procedure

LSU HCSD IT equipment and/or media shall only be disposed of by the facility IT Director or their designee in accordance with the State of Louisiana Office of Technology Services' Data Sanitization – Standards and Requirements (See Appendix D). IT equipment and/or media owned by an LSU HCSD facility which is to be reassigned to another employee or reused shall be examined by the facility IT Director, or their designee, and any protected or restricted information purged in accordance with these standards prior to reassignment and/or reuse.

LSU HCSD IT equipment must be properly stored throughout its lifetime, protecting it and its data from loss or theft. Equipment awaiting repurpose, surplus or destruction must be kept in a secure location.

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.

LSU HCSD Policy / Procedure

Note: This section is written with the clear understanding that the LSU HCSD network is an integral part of the LSUHNO network. Due to this relationship many procedures include use of the LSUHNO Department of Information Technology staff and equipment.

LSU HCSD has developed and implemented the following procedure for documenting and responding to significant information system incidents that impact multiple users.

An information security incident is any use or attempted use of LSU HCSD information technology assets in violation of federal, state laws, regulations, or LSU HCSD policies.

LSU HCSD shall maintain a Hospital/HQ (facility) Incident Response Team (HIRT). Information security incidents that impact multiple users shall be responded to by the HIRT. LSU HCSD shall maintain an email distribution list (HCSD Incident Response Team) consisting of all members of its HIRT and LSUHNO Enterprise Information Security Group. If a significant security incident is discovered at a LSU HCSD facility, the facility IT Security Officer or Privacy Officer shall immediately notify the HIRT via the email distribution list. If a significant security incident involving LSU HCSD is discovered by LSUHNO Department of Information Technology staff, the Enterprise Information Security Manager or designee shall immediately notify the HIRT via the email distribution list. The LSUHNO Enterprise Information Security Manager will determine if activation of the LSUHNO Computer Services Incident Response Team (CSIRT) is required.

Incident Response Team Memberships

HIRT Membership

- i. Privacy Officer at location of incident (Chair)*
- ii. IT Security Officer at location of incident*
- iii. LSU HCSD HQ IT Security Officer*
- iv. LSU HCSD Senior Attorney*
- v. LSUHNO Enterprise Information Security Manager*
- vi. Other personnel as deemed appropriate*

CSIRT Membership

- i. LSUHNO Enterprise Information Security Manager (Chair)*
- ii. LSUHNO Emergency Response Team*
- iii. IT Security Lead at location of Incident*
- iv. Internal Counsel*
- v. Compliance Officer at location of incident*

As specific security incidents warrant, department directors related to the location or staff involved in the incident and other personnel deemed necessary will join the HIRT at the request of the chair.

Information Security Incident Categories

Information security incidents can be categorized as follows:

- i. Unauthorized access – An individual or group gains or attempts to gain access to LSUHNO IT resources without authorization.
- ii. Denial of Service – An individual or group coordinates Internet traffic directed at LSUHNO IT resources such that legitimate use of the resources is adversely impacted.
- iii. Malware – 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 IT resources and compromise the security of protected information.
- iv. Criminal use – Use of any IT resource, whether LSUHNO or personally owned, on LSUHNO premises or via the LSUHNO network, which violates Federal or State law.

Incident Response Procedures

Information Security incidents are responded to as follows:

Incident Response Detection

Indicators of security incidents may include, but are not limited to, the following:

- i. Alert from Malware Incident Tracking System (M.I.T.S.)
- ii. Report to the Help Desk.
- iii. Report to a Computer Supporter.
- iv. Report from an outside agency.
- v. Alert from monitoring software (Antivirus, IDS, etc.)
- vi. Review of system logs.
- vii. Review of Internet traffic logs.
- viii. Malfunction.

Containment, Eradication, and Recovery

A. Priorities - In responding to a security incident the following priorities shall be observed:

- 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. Containment strategy

- i. Affected systems shall be isolated and countermeasures applied.
- ii. Users shall be kept up-to-date with expectations as appropriate.

C. Evidence collection

- i. Compromised systems or systems believed to contain evidence shall be isolated from the network but not shut down.
- ii. If an LSUHNO faculty, staff, student, or external user is suspected as a perpetrator of a criminal act the following additional data shall be collected, as dictated by the particular incident:
 - a. The files in the user's home directory.
 - b. The messages in the user mailbox.
 - c. System logs.

D. Recovery steps

- i. Remove inappropriate and/or unauthorized material.
- ii. Terminate unauthorized access.
- iii. Restore data from backups.

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

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.

LSU HCSD Policy / Procedure

Logon/ Logoff procedures shall be strictly followed. No person having been given access privileges to the LSU Health System Network, or information systems shall share their logon password with any other person. No person shall use their logon password to enable access for another person to a system for which that person does not have logon privileges. No person shall use another's logon password to gain access to a system. When a user leaves a computer workstation unattended where an information system is running that required the user to logon, the user must logoff the system or ensure the workstation is appropriately secure.

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.

LSU HCSD Policy / Procedure

All deliberate damage to, or theft of LSU HCSD IT property, information, or systems, or identification of any potential threat to such property, information or systems, shall be reported immediately to the IT Security Officer and the Compliance Officer at the location of incident and appropriate law enforcement as soon as it is discovered. In addition, notification shall be made to the Office of the Legislative Auditor and local District Attorney in accordance with HCSD Policy 2523.

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.

LSU HCSD Policy / Procedure

Department directors and supervisors, when requesting or approving access to information and systems for their employees shall ensure all access to information and systems is based on the lowest level of privilege needed for each employee to appropriately perform his or her job duties.

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.

LSU HCSD Policy / Procedure

Each employee, faculty, staff, student and/or contractor shall be assigned a unique user ID to access information systems.

Procedure for granting Access to Applications Containing Electronic Protected Health Information (ePHI)

PURPOSE

To provide a process for the health care facilities and external affiliates with the LSU HCSD to secure access for individual workforce members that use the LSU HCSD systems containing ePHI in order to perform job related activities. Each LSU HCSD facility and external affiliates will use this process to secure access for its individual users to the HCSD systems containing ePHI.

DEFINITIONS

Coordination and Communication of Information Sharing Committee (CCIS) – a committee comprised of LSU HCSD and the LSU System Partner Hospitals that monitor the security of the shared electronic systems that contain protected health information, as well as establish a consensus in processes and policy related to those systems.

ePHI systems – any application that stores electronic protected health information. Examples of such systems include Epic, CLIQ, RIS/PACs, etc.

Security Approver – Persons designated by LSU HCSD or external affiliate that is responsible for final approval of access to a particular LSU HCSD ePHI system.

Example: Document Imaging security approvers are Wil Dourrieu and Megan Moran.

Security Grantor – Persons responsible for assigning security permissions approved by the security approver.

Example: Document Imaging security grantors are Enterprise Information Security.

External Affiliate – External Affiliates are users who require access to LSU HCSD computer resources, but are not LSU HCSD employees. Computer access for External Affiliates must be authorized by and coordinated through an affiliate sponsor for each different external affiliation.

External Affiliate Sponsor – Persons responsible for coordinating with Enterprise Information Security on all matters relating to the affiliation.

Protected Health Information (sometimes referred to as “PHI”) – for purposes of this policy means individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. It includes demographic data that relates to that relates to:

The individual’s past, present, or future physical or mental health or condition;

The provision of health care to the individual; or

The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

PHI includes many common identifiers such as name, address, birth date, social security number, etc.

PROCEDURE

Granting of Initial Access

(See flow chart below)

1. A Security Approver will be designated for each HCSD system containing ePHI. The Security Approver will be responsible for the final approval of individual user’s access to the ePHI system.
2. Whenever an individual user requires access to an ePHI system, the user’s supervisor or External Affiliate sponsor will send a request for access to the Security Approver outlining the need for access to the ePHI system, including the job function that requires such access. The request shall be for the minimum necessary access to allow the required job function.
3. The Security Approver will review the request for access to determine if the access should be granted, and if so, the type of access that is appropriate.
4. If approved, the Security Approver will forward the request for access to the ePHI system’s Security Grantor, or if specific training is required prior to granting access to the ePHI system, the Security Approver will forward the request to the training team. Once all required training is completed the trainer will forward the request to the Security Grantor.
5. If the Security Approver does not approve the access, or needs additional information in order to process the request, the Security Approver will contact the requesting supervisor or External Affiliate Sponsor to request the additional information, or notify them of the denied request.
6. The Security Grantor will process the request to grant the user access to the ePHI system and notify the Security Approver and user’s supervisor of the access granted.

Transfers

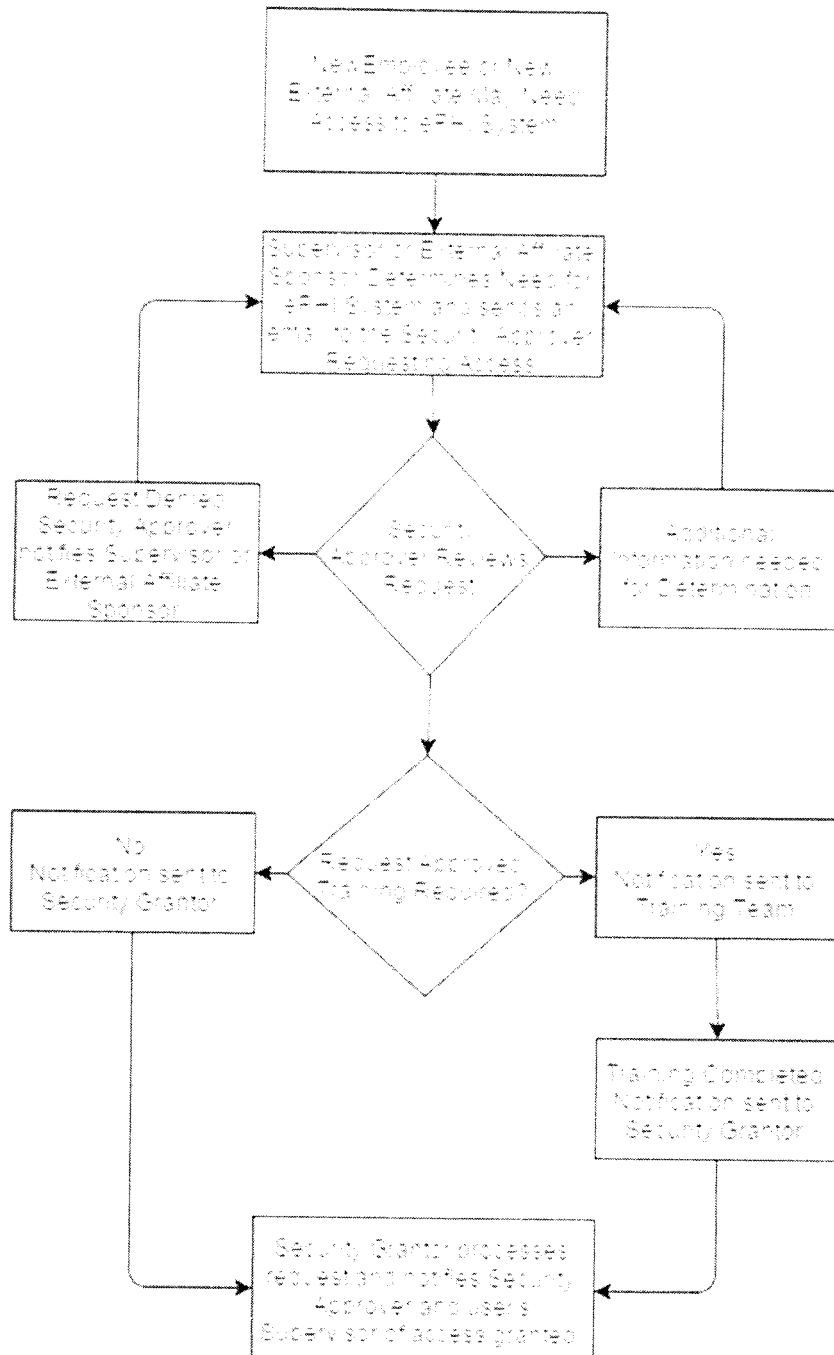
Each LSU HCSD facility and External Affiliate sponsor will designate a process whereby employees who transfer to another position or department will have their access to ePHI systems reviewed.

The steps of granting initial access should be followed when a change in access is needed due to a transfer so that the Security Approver has the opportunity to review the individual user’s job function to ensure the most appropriate access is granted.

Terminations

It is the responsibility of each LSU HCSD facility and External Affiliate sponsor to insure that all employees who are no longer affiliated with their facility have access to ePHI systems removed upon termination.

Each LSU HCSD facility and External Affiliate sponsor will develop a process to provide notification of termination to the Security Grantor of each ePHI system for which the terminated employee had access.



Security Approvers/Grantors for ePHI Systems

A table listing Security Approvers and Grantors can be found at:
http://www.lsuhsospitals.org/it_help_desk.aspx

When generic IDs are required by operational necessity for accessing systems containing protected or restricted information, the system owner working in conjunction with the facility IT Director and LSUHNO Information Security will document in writing the reason for the generic access, how such access will be granted, revoked, acceptable duration of access, and the method of auditing such access. LSU HCSD has adopted the LSUHNO standards and methods for generic ID as outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Enterprise Computer Services.

Policy Statement 2.1.3 – Securing Unattended Workstations

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

LSU HCSD Policy / Procedure

Precautions shall be taken to prevent access and tampering with unattended equipment, including but not restricted to desktop and portable computers, printers, network electronics and circuits, removable media devices and other equipment, by unauthorized persons in accordance with LSU HCSD HIPAA safeguards.

It is the responsibility of department directors, working in conjunction with their facility IT Director, to ensure all equipment in their business areas is placed in appropriately secure locations. In any business area where it is necessary to have equipment but where physical security of the equipment is determined to be at increased risk (i.e. areas that are not at all times occupied by LSU HCSD personnel), additional precautions should be taken to secure equipment in the work area. Protected or restricted information shall not be stored on a computer in a public use or untenable area.

It is the responsibility of department directors, and all employees, to ensure computer screens (monitors) containing restricted or protected information be placed so they are not visible to unauthorized persons. Where it is impossible to protect the peripheral view of computer screens that may contain restricted or protected information, screen privacy filters shall be employed.

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.

LSU HCSD Policy / Procedure

Access to LSU Health System Network equipment shall be strictly controlled to prevent unauthorized access or tampering with network electronics and network circuits and the transmission of data over such equipment. LSU HCSD has adopted the LSUHNO standard for network access controls outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Enterprise Computer Services.

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.

LSU HCSD Policy / Procedure

Access to the application supervisor and/or administrator commands shall require authorization from the employee's supervisor for whom the access is being granted and the owner of the application (system owner). Access to the operating system supervisor and/or administrator commands shall be restricted to those persons who are authorized to perform systems administration/management functions as determined by the facility IT Director or the HCSD CIO.

Policy Statement 2.1.6 Managing Passwords

All LSU information systems using passwords as the primary method of user authentication shall require all user accounts to 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 campuses 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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO standard for password length, password change interval, password complexity outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Enterprise Computer Services. The LSUHNO password standard will be implemented in applications that are capable of supporting the standard.

EIS 100

B.5 Password Policy

LSUHNO Password Policy requires that:

- i. Minimum password length and format shall be no less than ten (10) characters.
- ii. Minimum password complexity shall 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 (%,&,!).
- iii. Maximum validity periods for passwords to be no greater than 70 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.

LSU HCSD Policy / Procedure

Physical access to server rooms and network infrastructure closets shall be strictly controlled to prevent unauthorized access or tampering with server hardware, network equipment, communication equipment, application software, uninterrupted power and emergency power equipment, etc. stored in such environments. It is the responsibility of the facility IT Director (or his/her designee) to ensure appropriate physical safeguards are in place to prevent unauthorized access to each of these environments in the respective facility. Strong authentication and identification techniques shall be used in addition to physical safeguards 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 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.

LSU HCSD Policy / Procedure

Each LSU HCSD system owner, working in conjunction with the facility IT Director is responsible to ensure each LSU HCSD information system containing protected, and/or restricted information is configured to log the information necessary to detect and record attempts of unauthorized access, or system errors to the extent the logging facility exists and is capable. These logs shall be examined in a timely fashion by qualified staff. LSU HCSD has implemented the FairWarning privacy monitoring solution to assist with the monitoring of application audit logs. 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.

LSU HCSD Policy / Procedure

It is the responsibility of the system owner to determine the required level of access controls needed for the value and classification of the information assets being protected. The system owner, working in conjunction with the facility IT Director or the LSU HCSD CIO, and LSUHNO Enterprise Information Security, is responsible for establishing and implementing the required access controls prior to system deployment.

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.

LSU HCSD Policy / Procedure

Remote user access to LSU HCSD information and systems is controlled via the standards and methods outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology. These methods ensure accurate authentication of remote users, and the integrity and confidentiality of the information transmitted. These methods for accessing the LSU Health System Network remotely shall utilize a virtual private network (VPN), and/or Citrix ICA Connection.

EIS 100

All methods for accessing the LSUHNO network remotely shall use encryption and network account authentication to ensure the confidentiality, integrity, and availability of information transmitted during any session.

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.

LSU HCSD Policy / Procedure

In the event an LSU HCSD employee is incapacitated or unavailable and another employee must access a system to continue a required job function typically performed by the incapacitated/unavailable employee, and such access to the system is deemed emergent by the employees' supervisor(s) such that access cannot be delayed until the incapacitated/ unavailable employee is again available, access to the system will be granted according to the following: The employees' supervisor(s) request emergency access to the system by phone and written request (email) to the facility IT Director. The request must outline the reason such access is needed emergently, document that all required training for the requested access has been completed, and the duration for which the access is needed. The facility IT Director will review the request and/or contact the requestor by phone and/or by forwarding the email to the system owner, if applicable, for authorization. The facility IT Director will submit the authorized request by email with a follow-up phone call to LSUHNO Enterprise Information Security (or the EIS Analyst on call if after business hours), if applicable, to enable system access. Access is limited in duration and shall be terminated when the incapacitated/unavailable employee is again available, or when the requested duration for emergency access has passed, whichever comes first. For audit purposes, each instance of such access shall be documented and maintained on file by the facility IT director for a period of no less than six years, if the system or information accessed is protected or restricted 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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO Enterprise Networking Standards for configuring information system networks to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

Policy Statement 3.1.2 Managing the Network

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

LSU HCSD Policy / Procedure

Personnel responsible for managing the LSU Health System Network and preserving its integrity in support of LSU HCSD shall do so in accordance with the standards and methods outlined in LSUHNO EIS 100. LSU HCSD has adopted these LSUHNO standards to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

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 the system will not operate properly with the anti-virus software, appropriate information security safeguards shall be instituted.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the standards outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

EIS 100

All IT equipment shall incorporate all available mechanisms or safeguards to secure the LSUHNO network and network connected devices against both physical attack and unauthorized network intrusion. All servers and workstations shall be configured to LSUHNO standards (see Appendix A.)

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.

LSU HCSD Policy / Procedure

LSU HCSD shall appoint systems administrators who demonstrate the qualifications established by the division to manage the information technology systems and oversee the day to day security of these systems. Where LSU HCSD information technology systems and day to day security of these systems is managed for LSU HCSD by LSUHNO personnel, system administrators shall be appointed according to applicable LSUHNO Department of Information Technology hiring policies to support consistency and compliance with the network and application security infrastructure.

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.

LSU HCSD Policy / Procedure

LSU HCSD employees and affiliates shall be granted access to data based on the Minimum Necessary standard. Each LSU HCSD facility must identify the persons or groups in its workforce who need access to protected or restricted data to carry out their duties. Department directors are responsible for identifying such persons or groups and designating the types of protected or restricted data needed by each to carry out their duties. This designation should be based on the job duties of each person or group, and be granted using a role-based approach that delineates the category or categories of data each person or group requires.

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.

LSU HCSD Policy / Procedure

Third party access to LSU HCSD information or systems containing protected or restricted data shall be granted only after a contract is executed with the third party and the contract is accompanied by a signed Business Associate Agreement or comparable and applicable agreement, and a signed acknowledgement of the LSU HCSD Code of Conduct. In those situations where the need for third party access to LSU HCSD information or systems containing protected or restricted data is not accompanied by a contractual agreement (i.e. data sharing for the purpose of patient care continuity with community partner provider organizations), access to data shall be granted only after an information sharing agreement is in place and executed between LSU HCSD and the third party.

All LSU HCSD suppliers/vendors who handle protected or restricted information shall also acknowledge compliance with LSU HCSD information security procedures and LSU purchasing and procurement guidelines prior to the delivery of services.

The LSU HCSD BAA standard template can be found at:

<http://www.lsuhsospitals.org/docs/BA%20Contract%20lastREV614policyversion.doc>

Where information system and/or network access is required by a third party and a Business Associate Agreement is in place and executed, access to LSU HCSD information, systems shall be controlled via the standards and methods for "External Affiliates" outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

Policy Statement 3.2.4 – Ensuring Information Integrity

Each LSU System campus shall develop and implement procedures to ensure 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.

LSU HCSD Policy / Procedure

LSU HCSD shall document and implement the appropriate procedures within the Disaster Recovery Plan (DRP) to ensure the integrity of electronic protected, 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 facility management company engaged by a LSU System campus shall be expected to comply with LSU System Information Security policies and execute a Business Associate Agreement or similar document that communicates the performance expected and the remedies available in the instance of non compliance.

LSU HCSD Policy / Procedure

Any facilities management company engaged by an LSU HCSD facility shall comply with LSU HCSD Information Security policies and execute a Business Associate Agreement with the respective LSU HCSD purchasing and procurement department.

(Also see Policy Statement 3.2.3 – Permitting Third Party Access)

Subunit 3 – E-mail and the Internet

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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO Enterprise Networking Standards for configuring information system networks to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology. All faculty, staff, students, employees, vendors, and external affiliates shall abide by LSUHNO CM-42 and HCSD Internet policy 4512. CM-42 and HCSD 4512 provide guidelines to ensure information, software, and media downloaded from the Internet does not jeopardize the operations, reputation, or security of the LSUHNO and LSU 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 to require all email, 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 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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO standards and methods for digital communications generated by LSU HCSD information systems outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology. In addition to the basis provided by EIS 100, LSU HCSD email communications are controlled by the additional standards and methods outlined in the LSU HCSD Email Policy 4511, which prohibits any transmission of PHI via email.

EIS 100

Digital Communications

All forms of digital communication generated by LSUHNO 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. Protected or restricted information shall not be sent outside the LSUHNO information infrastructure without taking appropriate 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 malicious codes are not delivered to or executed on LSU information systems by receiving email and/or any other form of digital communication.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO standard for receiving electronic mail and other digital communications outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

EIS 100

Sending and Receiving Digital Communications

All inbound and outbound external and internal email shall be scanned for viruses on the email servers. The DIT may implement any procedures deemed necessary to ensure that malicious code is not executed on LSUHNO information systems by receiving digital communications.

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 to ensure emails and/or any other form of digital communication that contain protected or restricted information, including attachments, are correctly addressed and are 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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO standards and methods for digital communications generated by LSU HCSD information systems outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology. In addition to the basis provided by EIS 100, LSU HCSD email communications are controlled by the additional standards and methods outlined in the LSU HCSD Email Policy (4511).

Policy Statement 3.3.5 – Website Maintenance

Each LSU System campus shall develop and implement a procedure which ensures LSU System websites contain protected or restricted information are protected from unauthorized intrusion.

LSU HCSD Policy / Procedure

No employee or agent of LSU HCSD shall post restricted or protected information on a website, even if the website is protected from unauthorized intrusion by website security standards outlined in LSUHNO EIS 100, without the written authorization by the facility IT Director, the facility IT Security officer and the facility chief administrator. In those instances when the proper written authorization is obtained, LSU HCSD websites containing restricted or protected information shall be protected from unauthorized intrusion and tampering in accordance with website security standards outlined in LSUHNO EIS 100. LSU HCSD has adopted the LSUHNO website security outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

EIS 100

LSUHNO websites shall be protected from unauthorized intrusion and operated in accordance with LSUHNO EIS standards. Only designated personnel shall modify campus websites. All website modifications shall be documented.

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.

LSU HCSD Policy / Procedure

The transfer or exchange of restricted or protected data outside of LSU networks is only allowed when necessary to support a defined business purpose. When such transfer or exchange of data is required, it must utilize a secure method approved by LSUHNO Enterprise Information Security. Examples of secure methods are, encrypted VPN tunnel, Secure File Transfer Protocol (SFTP), and LiquidFiles. The facility IT Director should be consulted to determine the best method to transfer the data. Also see Policy Statement 1.3.1 – Using Removable Storage Media Including Diskettes and CDs.

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.

LSU HCSD Policy / Procedure

Data within LSU HCSD has many forms, Personally Identifiable Information (PII), Protected Health Information (PHI), Intellectual Property, Organization Proprietary and Non-Proprietary information. All employees whose work involves the use of this data, have the responsibility to protect this information.

The location where this data is stored varies by information system. It is the responsibility of the system administrators in conjunction with Information Technology, and LSUHSC Enterprise Information Security to manage access to this data. All access to data should be based on job function and minimum necessary standards.

No PII, PHI, Intellectual Property, or Organization Proprietary data should be stored on portable computing devices or removable storage media, unless for a defined business need and proper administrative approvals have been documented. See Policy Statement 1.3.1

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.

LSU HCSD Policy / Procedure

All LSU HCSD information systems containing protected or restricted information shall be protected by adequate backup and system recovery procedures. It is the responsibility of the system owner working in conjunction with the facility IT Director to ensure such protections are in place. Procedures for backup and system recovery should be documented in the facilities Disaster Recovery Plan.

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 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.

LSU HCSD Policy / Procedure

Each LSU HCSD facility shall make every effort to ensure all terms and conditions of End User License Agreements (EULA) for the software in use at the facility and by their employees 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 the campus' business is not compromised. Every effort shall be made to resolve software problems efficiently and within an acceptable time period.

LSU HCSD Policy / Procedure

All LSU HCSD application software shall be supported to ensure LSU HCSD business is not compromised. The facility IT Director shall make every effort to resolve software problems efficiently and within an acceptable time period to minimize any disruption to operations.

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.

LSU HCSD Policy / Procedure

LSU HCSD information systems software shall not be disposed of unless authorized in writing by the system owner and the department directors of those areas whose business needs are supported by the software. LSU HCSD information systems software shall not be entered into the “Disposition Phase” of the disposition plan unless it is determined by the system owner and the appropriate department directors the software is no longer required, and its related data can be archived.

The Disposition Phase represents the end of the systems life cycle. It provides for the systematic termination of a system to ensure vital information is preserved for potential future access and/or reactivation. The placement of a system into the Disposition Phase means it has been declared surplus and/or obsolete, and is scheduled to be shut down. The emphasis of this phase is to ensure 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, organization policies regarding retention of electronic records. Disposition actions should proceed according to the Disposition Plan outlined in Appendix C.

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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO EIS procedure for operational program libraries to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

EIS procedure

All operational program libraries for critical applications developed by LSUHNO or LSU HCSD shall reside on enterprise servers. Access to operational program libraries shall be controlled by the EIS and provided on an “as needed” basis.

The determination of “as needed” will be the responsibility of facility IT Director, the system owner and/or the LSU HCSD CIO. All changes to systems, source code and operational program libraries shall be documented in writing, properly authorized and tested before moving to the live environment.

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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO EIS procedure for program source libraries to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

EIS procedure

All program source libraries, executables, and linked libraries for critical applications developed by LSUHNO shall reside on enterprise servers. Access to program source libraries shall be controlled by EIS and provided on an as needed basis.

The determination of “as needed” will be the responsibility of the facility IT Director, the system owner and/or the HCSD CIO. All changes to systems, source code and program source libraries shall be documented in writing, properly authorized and tested before moving to the live environment.

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.

LSU HCSD Policy / Procedure

See Policy Statement 5.1.1 – Managing Operational Program Libraries and Policy Statement 5.1.2 –

Managing Program Source Libraries (above)

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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO Application Security Standards outlined in LSUHNO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology. All new applications shall adhere to the Application Security Guidelines (Appendix B).

Subunit 3 – Testing and Training Environments

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.

LSU HCSD Policy / Procedure

The use of protected or restricted data for testing of new systems or system changes shall adhere to the same policies and procedures established for systems and information already in production.

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.

LSU HCSD Policy / Procedure

System owners will work with the facility IT Directors, application vendors/developers, 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. The training plans shall include a detailed procedure by which users and technical staff are trained in the functionality and operations of the new application. Systems that have significant upgrades that include new processes for the users shall also require a training plan to familiarize the users with the changes.

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.

LSU HCSD Policy / Procedure

See LSUHNO CM 42. LSU HCSD 8501 and LSU HCSD 4539.

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.

LSU HCSD Policy / Procedure

See LSUHNO CM 42. LSU HCSD 8501 and LSU HCSD 4539.

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.

LSU HCSD Policy / Procedure

See LSUHNO CM 42. LSU HCSD 8501 and LSU HCSD 4539.

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 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.

LSU HCSD Policy / Procedure

Each LSU HCSD facility 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 these services are disrupted. A current copy of this plan and any amendments shall be submitted to the LSU HCSD Office of the Chief Executive Officer for review and to be kept on file. Each LSU HCSD campus is responsible for periodically reviewing and keeping the plan up-to-date.

Each LSU HCSD facility IT department shall follow procedures within the LSU HCSD IT Disaster Recovery Plan to ensure the continuation of key information services in the event these services are disrupted. The LSU HCSD IT DRP shall be reviewed no less frequently than every three (3) 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 (3) years.

LSU HCSD Policy / Procedure

Each LSU HCSD facility shall conduct a formal risk assessment in order to determine the requirements for the BCP/DRP. Each LSU HCSD facility shall review its risk assessment after each emergency and at least every three (3) 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.

LSU HCSD Policy / Procedure

Each LSU HCSD facility shall test the BCP/DRP (i.e. a disaster recovery drill) at least annually and follow the appropriate procedures regarding testing. The results of such testing shall be submitted to the LSU HCSD Office of the Chief Executive Officer. 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, LSU HCSD staff shall receive training in the use of the BCP/DRP and in their continuity plan roles.

LSU HCSD Policy / Procedure

Each LSU HCSD facility shall provide training in the use of the BCP/DRP to all appropriate LSU HCSD facility staff.

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

LSU HCSD Policy / Procedure

All LSU HCSD facilities shall require employees and students to acknowledge compliance with information security policies. Non-compliance with information security policies may result in immediate disciplinary action, up to and including termination of employment and/or enrollment. Compliance with information security policies is to be included in any “Terms of Employment” and the campus’ Code of Conduct.

Each LSU HCSD campus shall verify prior to hiring that new employees have not been sanctioned or excluded from participation in federal healthcare programs.

Human Resources shall ensure the Information Technology department is notified of all personnel actions (promotions, demotions, transfers within a facility or to other facilities, or terminations). Personnel actions may require a change in network, system or information access. The IT Director or designee in conjunction with the employees' supervisor will review any personnel actions to determine if any needed change in network, systems, or information access is required. The IT Director or designee will communicate any required changes in access to LSUHNO EIS and/or information system administrators. In the case of a termination, access is to be revoked as of the termination date. If in the judgment of the appropriate campus official, it is determined an employee represents a risk to the security of LSU HCSO information, all access shall be terminated immediately.

All new LSU HCSO employees, faculty, staff, and students shall receive Information Security training appropriate for their job function. Each new user shall complete the initial LSU HCSO HIPAA Privacy and Security training prior to being granted access to information. This education shall occur on an annual basis; however, if a user's job responsibilities change, training requirements shall be reassessed by the employee's department director or supervisor.

Updates on Information Security awareness shall be provided by the IT Security Officers and/or Compliance Officers to the staff as events warrant.

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.

LSU HCSO Policy / Procedure

See LSUHNO CM 42 LSU HCSO 7500, 8501, 4515, 4547, 4546, 4522, 4538, 4544, and 4539.

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.

LSU HCSO Policy / Procedure

See Policy Statements 1.4.1 – Contracting or Using Outsourced Processing, 2.1.2 – Managing User Access and 3.2.3 – Permitting Third Party Access

Lending of keys, both physical and electronic, is prohibited. In the event 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.

LSU HCSO Policy / Procedure

See Policy Statements 1.4.1 – Contracting or Using Outsourced Processing, 2.1.2 – Managing User Access and 3.2.3 – Permitting Third Party Access

The LSU HCSD BAA standard template can be found at:

<http://www.lsuhsospitals.org/docs/BA%20Contract%20lastREV614policyversion.doc>

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.

LSU HCSD Policy / Procedure

All LSU HCSD faculty, staff and students are expected to treat passwords as private and highly confidential. Sharing of passwords is strictly forbidden. See Policy Statement 1.6.3 – Logon and Logoff from Computer

Subunit 3 – Employment Termination

Policy Statement 8.3.1 – Staff Resignations

All LSU System campuses shall ensure 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 an employee represents a risk to the security of LSU System campus information, all access shall be terminated immediately.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO procedure for revoking access to LSU HCSD/ LSUHNO information systems to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology.

The IT Director at each site will contact LSUHNO 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 LSUHNO 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 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 LSU campuses. 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 disable the user's Active Directory account, and remove access to the identified systems. EIS will then notify the computer support group for the user 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.

LSU HCSD Policy / Procedure

See LSUHSC CM 42, LSU HCSD 7500, 8501, 4515, 4547, 4546, 4522, 4538, 4544 and 4539.

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.

LSU HCSD Policy / Procedure

All LSU HCSD temporary staff will abide by the same LSU HCSD Information Security policies and procedures as permanent staff, including acknowledgement of compliance with LSU HCSD Information Security policies prior to beginning work.

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.

LSU HCSD Policy / Procedure

Proposed changes or amendments to policies will be presented to LSU HCSD leadership for approval. Updated policies will be distributed to LSU HCSD facilities for implementation.

LSU HCSD will include Information Security awareness in annual orientation and updates will be communicated effectively throughout the organization. In all of the training, it will be emphasized the Compliance Officer/Privacy Officer or Security Officer must be notified if these policies are not followed.

Subunit 2 Training

Policy Statement 9.2.1 Information Security Training Appropriate to Job Function

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.

LSU HCSD Policy / Procedure

LSU HCSD staff whose job requires the use of facility and/or departmental information systems will receive security training specific to the information systems used. The training may be provided via training modules or as part of department orientation. The local system administrator in conjunction with the individual's supervisor is responsible to insure this training is completed.

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.

LSU HCSD Policy / Procedure

Standard LSU HCSD general Compliance and HIPAA Privacy training modules and LSU HCSD Information Security training modules have been developed to be presented to employees within the LSU HCSD HQ office and the hospitals by Compliance at General Orientation, Contracted Employee Orientation, and Medical Staff/Resident Orientation. The information presented is an overview of the intent of each section, with the stated expectation the employee/resident is to review the detailed LSU 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 the employee/resident received the material. These modules will be standard for the LSU HCSD.

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.

LSU HCSD Policy / Procedure

All LSU HCSD 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. Consideration of public viewing of data or access to hardware shall be taken during the placement of computer equipment. If a computer must be placed in an

area where public viewing of the computer screen is inevitable, a privacy screen must be installed.

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.

LSU HCSD Policy / Procedure

LSU HCSD has adopted the LSUHNO EIS procedures for defending against unauthorized or criminal activity to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHNO Department of Information Technology. Each campus shall configure all servers and workstation in accordance with the standards outlined in EIS 100 (Appendix A).

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.

LSU HCSD Policy / Procedure

LSU HCSD shall adhere to the LSUHNO Enterprise Information Security (EIS) and LSU HCSD Incident Response Procedure (See Policy Statement 1.6.2 – above).

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 for the thorough investigation of information security incidents as defined by the campus IT department. Investigators shall be properly trained and qualified. Results of the investigation shall be thoroughly documented in a security incident report to be kept on file for at least six years. The report shall include any and all recommendations to prevent recurrence of similar incidents.

LSU HCSD Policy / Procedure

LSU HCSD shall adhere to the LSUHNO Enterprise Information Security (EIS) and LSU HCSD Incident Response Procedure (See Policy Statement 1.6.2 – above). Results of the investigation shall be thoroughly documented in a security incident report to be kept on file for at least six (6) 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.

LSU HCSD Policy / Procedure

LSU HCSD shall adhere to the LSUHNO Enterprise Information Security (EIS) and LSU HCSD Incident Response Procedure (See Policy Statement 1.6.2 – above). 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.

LSU HCSD Policy / Procedure

See Policy Statement 1.2.1 – Supplying Continuous Power to Critical Equipment and Policy Statement 1.2.2 – Managing High Availability Systems.

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.

LSU HCSD Policy / Procedure

All LSU HCSD facilities shall maintain an inventory of their information assets, including electronic protected or restricted information that documents the rankings of each asset with regard to its level of confidentiality, sensitivity, integrity, availability and value.

See also Policy Statements 1.2.1 – Supplying Continuous Power to Critical Equipment and Policy Statement 1.2.2 – Managing High Availability Systems.

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.

LSU HCSD Policy / Procedure

For the purposes of LSU HCSD, the definition of protected information is extended explicitly to be inclusive of “protected health information” as defined by HIPAA regulations.

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.

LSU HCSD Policy / Procedure

For the purposes of LSU HCSD, the definition of restricted information is extended explicitly to be inclusive of “protected health information” as defined by HIPAA regulations.

Appendix A – Workstation and Server Standards

EIS

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 LSUHNO network. This document does not 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 (OS) they have chosen, the hardware on which it runs, and any applications they intend to install.

A.1 Workstation Standards

All workstations connected to the LSUHNO network shall be configured according to the following guidelines:

1. Workstations shall be configured to receive patches via an automated patching system such as WSUS or SCCM. All exceptions to this requirement shall be documented.
2. The OS shall be properly installed and configured and all relevant security patches for both the OS and all necessary applications shall be applied.
3. All unnecessary services shall be disabled (e.g. HTTP server, Telnet server, FTP server, SMTP server, DNS server, etc.). Only those services which are necessary for maintenance or to accomplish the task assigned to a workstation shall be enabled.
4. All services running on a workstation shall be patched and secured properly before being enabled.
5. No workstations are allowed to run DNS or DHCP server services under any circumstances.
6. All default passwords shall be changed immediately and shall be in accordance with LSUHNO password policy. Passwords shall not be stored unencrypted.
7. Access to administrator passwords shall be limited to the smallest number of people necessary to properly maintain the workstation and to allow access in case of emergencies.
8. Accounts with administrative access to the workstation shall not be used for routine work. A separate account shall be used for administrative access and utilities such as “su”, “sudo”, or “runas” shall be used when administrative access is required.
9. Virus and spyware protection shall be properly installed, configured, and updated.
10. Every workstation shall use a dynamically assigned IP address. If the workstation requires a static IP address, the computer supporter shall consult with LSUHNO Department of Information Technology (DIT) to establish the requirements.
11. If the OS provides a stateful firewall (e.g. Windows Firewall, ipchains, iptables, ipfw, etc.), it shall be enabled and only outgoing traffic shall be allowed with limited exceptions for remote management and vulnerability scanning.
12. All workstations shall have access logging enabled.

A.2 Server Standards

All servers connected to the LSUHNO network shall be configured according to the following guidelines:

1. Servers shall be configured to receive patches via an automated patching system such as WSUS or SCCM. All exceptions to this requirement shall be documented.
2. The OS shall be properly installed and configured, and all relevant security patches for both the OS and all installed applications shall be applied.
3. All network application services not essential to the prime function of the server shall be disabled. No services shall be enabled unless they have been patched to current levels and are necessary to accomplish the task assigned to a server.
4. No servers are allowed to run LDAP, DNS, DHCP, or Windows Directory Services without prior coordination with LSUHNO DIT.
5. Servers shall be located in designated server rooms or secured locations.
6. All default passwords shall be changed immediately and shall be in accordance with LSUHNO password policy. Passwords shall not be stored unencrypted.
7. Access to administrator passwords shall be limited to the smallest number of people necessary to properly maintain the server and to allow access in case of emergencies.
8. Server administrators shall supply accurate contact information to LSUHNO DIT for emergencies such as power outages and server breakins. This information shall also include a general description of the server, its purpose, and any special requirements or configuration.
9. Virus and spyware protection shall be properly installed, configured, and updated whenever supported by the OS.
10. Every server shall be plugged in to an Uninterruptible Power Supply (UPS).
11. Every server shall have an appropriate name, static IP address, and DNS record.
12. All servers shall be administered by qualified personnel.
13. If the OS provides a stateful firewall (e.g. Windows Firewall, ipchains, iptables, ipfw, etc.), it shall be enabled and only those ports necessary to allow the server to function, allow remote management, and allow vulnerability scanning shall be open.
14. Logging shall be enabled on all enterprise production servers and logs shall be forwarded to a centralized logging system.

A.3 Vendor Managed Systems

All vendor managed systems connected to the LSUHNO network shall be configured according to the following guidelines:

1. Owners of equipment managed by vendors shall consult with LSUHNO EIS regarding special needs before connecting to the network. This equipment may include special instrumentation (e.g. mass spectrometers, electron microscopes, specialized medical equipment, etc.), application software that requires a certain Service Pack or patch level and cannot be patched to current levels, FDA approved equipment which cannot be altered in any way without losing FDA approval, or similar types of equipment where the vendor or some other non-LSUHNO entity controls what patching may be done to such equipment.
2. Consideration shall be given to both internal and external threats for equipment that falls under specific federal or state regulations.
3. All information technology equipment used for research funded by grants must be in compliance with Federal, State, and LSUHNO guidelines.
4. LSUHNO password policy shall be enforced on all accounts used on vendor managed equipment.
5. Vendor managed equipment shall follow best practices for OS and application security.

Appendix B – Application Security Guidelines

Below are general guidelines for security requirements for an application:

- Must support AD as authentication provider using full LDAP or native integration. It is the preferred method of logging on to the application. Therefore Windows, not the application, would control password policy.
- User accounts should be setup in the application. Security groups should be assigned to user accounts to control access. Security groups should be configurable, the more granular, the better. A change to a Security group would affect all users assigned to the group. Should support the mapping of application security groups to Active Directory groups via LDAP or native AD integration.
- Users should only be able to access the data through the application.
- Separation of duties between System Administrators and Security Administrators. Security related functions should be restricted from all other users, including System Administrators.
- Application should support row level security to allow for the control of access to data, e.g. department, hospital, business unit, etc.
- Auditing – mandatory for clinical applications. Logon/logoff, changes to security, browse and changes to data.
- The application should stop if the user fails to enter a valid userid and password (3-5 tries).
- Automatic logoff due to inactivity
- Externally hosted applications must authenticate with LSUHSC credentials using RADIUS

Questions for Application Security

Below are general questions for security requirements of an application:

- 1.1.1 Describe how your application integrates with Microsoft Active Directory (LDAP authentication). Are schema changes required? Does it provide failover functionality? Can it be configured using port 389 and 636(SSL)?
- 1.1.2 Describe how users are granted access to the application. What flexibility is provided? What ability does the customer have to define security classes that combine view only, update and approval options?
- 1.1.3
 - a. Are security groups used?
 - b. Are the security groups customizable?
 - c. How granular are security groups?
 - d. Do changes to a group automatically affect all users in the group?
- 1.1.4
 - a. Describe how users are granted access to the data. Must users have database logins?
 - b. If so, how do these logins relate to the user's NT User ID?
- 1.1.5 Describe how row level security is implemented.
- 1.1.7 Does your application support separation of duties between System Administrators and Security Administrators?
- 1.1.8 Describe auditing and logs. Is Logon/logoff logged? Are changes to security logged? Are changes to data logged? Is reading data logged?
- 1.1.9 Does the application support automatic inactivity logoff?
- 1.1.10 Does the application close if the user fails to enter a valid userid and password after a given number attempts?
- 1.1.11 Does installation require service accounts? If so, can the service accounts be renamed and can their password be changed?
- 1.1.12 Externally hosted applications must authenticate with LSUHSC credentials using RADIUS.
- 1.1.13 Are there delivered accounts in the software? Can the password be reset? Are they subject to LDAP if that is enabled on the software?

Appendix C – Disposition Plan

The practice of Disposition is the final phase of the system life cycle. It involves either the transitioning of information, hardware, software, and documentation from the current system to another system, or the archiving or destroying of it. Each must ensure that the transition of the various components is done in an orderly fashion and ensures the confidentiality, integrity, and possible availability of the information in the future. It involves planning for the possibility of having to reinstall and bring the system back to an operational status, if necessary, and to preserve the data so it is effectively migrated to another system or archived for potential future access. The practice also ensures that media is properly sanitized, and that hardware and software is disposed of in conformance with all relevant legal and IT Security requirements.

The practice of Disposition consists of three main activity groups:

Information Preservation – Ensures that information is retained in a usable format. Information can be transferred to another system, or archived. When archiving, consider what retrieval method will be used in the future to access the data. The retrieval method that is currently used may not be available in the future. Also consider what type of encryption should be applied for long term storage. In addition, you will need to consider the legal requirements for records retention.

Media Sanitization – Ensures that the data is irretrievable from the retired storage media. Different categories of sanitization can provide different levels of protection for your data. LSU HCSD Data Sanitization Standards and Requirements provide approved methods of sanitization.

Hardware and Software Disposal – Ensures that the hardware and software are disposed of in accordance with HCSD requirements. Data contained in full or partial files can include potentially sensitive information. Since it is still on the drive, it can be recovered using commercially available software. It is essential that sanitization is performed on the system components prior to the disposal of the hardware and software to protect the confidentiality of the information. The disposition of software needs to be in keeping with its license or other agreements, if applicable. Some licenses are site specific or contain other agreements that prevent the software from being transferred.

Planning during this phase of the systems life cycle is as important as any other even though it is often the last major process of a system's life.

The key elements of Disposition are:

1. **Gather Stakeholder Impact Input**

Communicate with different stakeholder communities that most use the system. Determine the current usage of the data, functionality of the system and nature of the usage (mission critical, very useful, marginally useful, or optional). Also consider whether other systems can absorb the data or functionality that is still heavily used. In addition, be sure to identify any technical interdependencies with other systems which may need to be addressed.

2. **Communicate Decision to Stakeholders**

Draft an initial communication for distribution to the stakeholder community. If different potential audiences are likely to have different priorities in regard to the system disposition, then the communication should be customized to address the unique sensitivities of the different audiences. This communication should be reviewed and approved by appropriate management. At a minimum, the contents of this initial communication should include:

- The rationale for disposing of the system
- The plan for transitioning any data of functionality that will be retained.
- The tentative timeline for disposition.

3. Prepare and Review Disposition Plan

Prepare a system specific draft disposition plan. This plan should be reviewed and approved by appropriate management and stakeholders.

4. Communicate Schedule to Stakeholders

Prepare a second communication that is customized to address the different stakeholder audiences identified earlier. At a minimum, it should include the planned schedule for the system disposition and any planned outages that will occur during the disposition. This communication should be reviewed and approved by appropriate management.

5. Archive System Data and Documentation

Transfer the following items to the archive specified in the Disposition Plan:

- A complete copy of all system data.
- A complete copy of all system documentation.
- A copy of any external software that is required for proper system operation.
- Transition any data that is to be absorbed by other systems to those systems.
- Transition any ongoing operations to other systems.
- Take the system that is being disposed offline.

6. Dispose of System

Transition any ongoing operations to other systems and take the system offline. Process any dedicated system hardware in accordance with data sanitization and requirements.

7. Disposition Review

Review all planned disposition activities to insure all have been completed.

8. Notify Stakeholders that Disposition is Complete

Draft the final communication for distribution to the stakeholder community to notify them that the disposition is complete. This communication should be reviewed and approved by appropriate management. The communication should include at a minimum the following:

- Official confirmation that the system has been retired.
- Overview of how the "retired" functionality has been replaced by other systems.

Disposition Plan Checklist

Initial System Evaluation & Planning

Has all system information been assigned a security categorization?

Have plans for re-use and/or recycling of media, hardware, and software been determined?

Has a formal system disposition plan that documents all required activities been completed?

Has the impact of system disposition on system stakeholders been assessed?

Have all technical interdependencies with other systems been identified, and mitigation strategies documented?

Communications

Has all system documentation been removed and/or updated to reflect the disposition of the system?

Has the user community been notified of the schedule for system disposition?

Data Disposition

Has all system data been archived in the agreed-upon format?

Has all system data been evaluated to identify all applicable legal requirements for records retention?

Has archival data been stored in a "save forever" backup area?

Software Disposition

Have all software library files related to the information system been archived, deleted, or transferred to other systems, as planned?

Documentation Disposition

Has a copy of all current information system documentation been archived in an agreed-upon format?

Have all system procedures been archived in an agreed-upon format?

Have all system procedures and documentation been stored in an agreed-upon archive location?

Equipment Disposition	
	Has all electronic media been sanitized, as appropriate, for the assigned information security categorization and recycling/reuse plan?
	Has media sanitization been validated and documented?
	Have the hardware and software resources dedicated to this information system been completely documented?
	Is a reuse, recycling, or destruction plan documented for all system hardware and software resources?

Appendix D – Data Sanitization – Standards and Requirements

All LSU HCSD facilities will abide by the State of Louisiana Office of Technology Services Data Sanitization Standards and Requirements as attached on the following page.

Data Sanitization – Standards and Requirements

Explanation

Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying data stored on a device or electronic media. A device that has been successfully sanitized has no residual data even when data recovery is attempted with advanced forensic tools.

Purpose

The purpose of this document is to empower all applicable entities with a clear list of acceptable methods, options, and corresponding instructions to produce consistent reliable results when Data Sanitization is required.

Approved Sanitization methods are listed where available and only apply to the assigned media type in the Process Requirements section. The sanitization procedure selected should be the option that best suits the operational needs of the Agency or entity.

Scope

Any electronic device or media owned, managed, leased or utilized by the State Offices of Louisiana with the ability to store, process, or transmit internal, Confidential, or Restricted Data (See OTS Data Classification Policy). Examples include, but not limited to, Hard Drives, CDs, Backup Tapes, USB Drives, Smart Phones, Tablets, Fax Machines, Routers, Firewalls, VOIP Handsets, Network Storage Devices, and Printers.

The following requirements should also be referenced when specifying Data Sanitization requirements for contracted Partners or Service Providers storing or processing State Data.

Sanitization Requirements

There are only three acceptable approaches for data sanitization: Clearing, Purging, and Destruction. Each method has its own requirements, considerations, and approved processes.

- **Destruction**
 - Approved methods:
 - o Shred (Printed Material Only – see Approved Processes)
 - o Pulverize
 - o Melt
 - o Incinerate or Disintegrate
 - Additional Requirements:
 - o Sanitization Log (see Log Requirements)
 - o Use of an approved process or partner
- **Purging**
 - Approved methods:
 - o Degaussing
 - Additional Requirements:
 - o Sanitization Log (see Log Requirements)
 - o Use of approved and serviced equipment
- **Clearing**
 - Approved methods:
 - o Overwrite (Single or Multiple Pass)
 - o Factory Reset
 - o Removing Power
 - Additional Requirements:
 - o Sanitization Log (see Log Requirements)
 - o Only approved procedures and software are to be used. (see Process Requirements)
 - o Overwrite Procedures must be documented, validated, and approved prior to Agency use on production equipment.

See Process Requirements section to follow the required sanitization process for specific Device or Media type

Data Sanitization – Standards and Requirements

Log Requirements

Each time data sanitization is attempted (success or failure) a Sanitization Log record must be created.

Each Sanitization Log record must contain the following fields of information:

- **Media or Device Type**
- **Sanitization Status Code** (see Process section below)
- **Manufacturer unique ID** (Ex. Hard drive Serial Number)
- **Date and Time of Sanitization**
- **Full Name of individual that performed the sanitization**

Sanitization Logs may be created and maintained manually or by an application or system.

If an Agency or entity does not have a preferred Sanitization Log format, the attached OTS Sanitization Log should be used.

When preparing equipment for LPAA surplus or disposal, the LPAA Sanitization Certificate form should be used in place of the OTS Sanitization Log. See: LPAA POL 201401

*In cases where an approved Third Party or Partner is performing the sanitization process, the "Sanitization Status Code" may be substituted for "Sanitization Method" and "Status" (Success or Failure).

Please contact OTS Information Security with any questions related to Third Party sanitization.

Process Requirements

Each known device or media type is listed below with the steps required to ensure all data has been removed prior to disposal or surplus.

Following each process will produce a "Sanitization Status Code" required for the Sanitization Log.

Prior to any sanitization actions the following considerations should be made:

- **Data Retention Requirements**
 - Agency staff should ensure that performing data sanitization does not violate any Agency directive or legal obligation to retain data. (Ex. "Legal hold")
- **Work Area**
 - Ensure resources performing the sanitization have an organized and controlled work area to ensure devices or media are not accidentally mixed with similar production devices or media.
- **Inventory**
 - If bulk sanitization is required, an initial inventory should be taken (and updated as needed) of the devices or media to ensure all devices or media is accounted for throughout the sanitization process.
 - Once sanitization is complete, a final count should be completed to confirm all devices or media are accounted for and have been successfully sanitized.

Data Sanitization – Standards and Requirements

Approved Processes

If an Agency, entity, or OTS resource identifies a device or media type not listed below, please contact [OTS Information Security](#) to request guidance for approved sanitization process. Please make sure to include manufacture, description, and explanation of the device or media function in a specific business process.

- **Hard Copies - (Printed Material)**
 - All Printed Material containing Confidential or Restricted Data must be destroyed using one of the following specifically approved destruction methods:
 - o Shred
 - Using cross cut shredders which produce particles that are 1 x 5 millimeters in size (or smaller)
 - o Pulverize or Disintegrate
 - Using disintegrator devices equipped with 3/32 inch security screen.
 - o Incinerate (Burn)
 - Material residue must be reduced to white ash.

- **CD, DVD, or BD - (Optical Media)**
 - For all Optical Media Discs:
 - o Destroy disc using approved destruction methods (see Sanitization Requirements).
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **OMDS**

- **Desktop or Laptop - (Workstations)**
 - Any:
 - o Workstation that has joined a state domain and had a user login must be sanitized prior to surplus or disposal.
 - o Test workstation or "Lab equipment" used to process, store, or transmit any state data.
 - For devices containing a single Hard Disk Drive (HDD) or Solid State Drive (SSD):
 - o **Use HDD or SSD process below.**
 - For devices containing multiple internal HDDs or SSDs:
 - o Extract each drive
 - o **Use HDD or SSD process below.**

- **Fax Machine - (Facsimile)**
 - For working devices that only perform facsimile functions:
 - o Power on device and perform a factory reset via menu or manufacture instructions.
 - o If completed successfully, label device with LPAA label.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **MRS**
 - o If the device does not have a reset option or does not complete the reset successfully,
 - **Follow process for broken device (below).**
 - For broken devices that only perform facsimile functions:
 - o Destroy Device using approved destruction methods (see Sanitization Requirements).
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **DS**
 - For devices that perform fax, printer, and copying functions:
 - o **Use Multifunction Device (MFD) process below.**

Approved Processes (Cont.)

- **Printer, Scanner, Copy Machine, or Multifunction Device (MFD) - (Office Equipment)**
 - For devices containing a Hard Disk Drive (HDD) or Solid State Drive (SSD):
 - o **Use HDD or SSD process below.**
 - For operational devices that do not contain HDD or SSD internal storage:
 - o Contact Manufacture (by email, phone, or website) for the steps required to clear all data for the specific device model.
 - o If completed successfully, or does not contain data, label device with LPAA label.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **MRS**
 - For working or broken devices that do not store or cache data:
 - o Label device with LPAA label.
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **ND**
 - For broken or damaged devices that have been confirmed to or expected to store or cache data:
 - o Destroy Device using approved destruction methods (see Sanitization Requirements).
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **DS**

- **Firewall, Router, or VOIP Handset - (Network Devices)**
 - For operational devices:
 - o Contact Manufacture (by email, phone, or website) for the steps required to perform a factory reset.
 - o If reset completed successfully:
 - Label device with LPAA label.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **MRS**
 - o If reset failed:
 - Create Sanitization Log Record.
 - Sanitization Status Code: **MRFMD**
 - **Follow process for broken or damaged device.**
 - o If reset is not available:
 - **Follow process for broken or damaged device.**
 - For broken or damaged devices:
 - o Destroy device using approved destruction methods (see Sanitization Requirements).
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **DS**

- **Portable USB Drives or Memory Cards - (Removable Media)**
 - For all:
 - o Destroy disc using approved destruction methods (see Sanitization Requirements).
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **RMDS**

Approved Processes (Cont.)

- **Hard Disk Drives - (HDD) or Solid State Drives - (SSD) - SCSI, IDE & ATA (SATA, eSATA)**
- For an operational drive:
 - o An approved OTS Overwrite Standard Operating Procedure (SOP) must be followed:
 - OTS-InfoSec-SOP-101
 - OTS-InfoSec-SOP-102
 - If an Agency or OTS resource prefers to utilize an alternate Overwrite procedure or solution:
 - The alternate procedure must be documented (see OTS SOP for format).
 - The proposed procedure must be sent to OTS Information Security for review and approval.
 - Written approval must be obtained from OTS Information Security prior to utilizing any alternative overwrite procedures or solutions for sanitizing any production drives.
 - o If an approved Overwrite procedure completed successfully:
 - If applicable, make sure to correctly place drive back in the correct parent device.
 - Label device with LPAA label.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **OWS**
 - o If approved Overwrite procedure failed:
 - Create Sanitization Log Record.
 - Sanitization Status Code: **OWFMD**
 - **Follow process for damaged or inoperable drive.**
- For a damaged or inoperable drive:
 - o If HDD:
 - The Drive may be Degaussed (if equipment is available) or Destroyed.
 - If Degaussed is preferred:
 - Degauss.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **OWFDGS**
 - Label original (parent) device with LPAA label.
 - If Destruction is required:
 - Destroy drive using approved destruction methods (see Sanitization Requirements).
 - Create Sanitization Log Record.
 - Sanitization Status Code: **OWFDS**
 - Label original (parent) device with LPAA label.
 - o If SSD:
 - Destroy drive using approved destruction methods (see Sanitization Requirements).
 - Create Sanitization Log Record.
 - Sanitization Status Code: **OWFDS**
 - Label original (parent) device with LPAA label.

Data Sanitization – Standards and Requirements

Approved Processes (Cont.)

- **Smart Phone, Tablet, or PDA (Ex. iPhone, Blackberry, iPad, etc.) – (Mobile Devices)**
 - For operational devices:
 - o Perform Full System Reset or contact Manufacture (by email, phone, or website) for the steps required to perform a FULL factory reset.
 - o If reset completed successfully:
 - Manually spot check device to ensure all photos, documents, history was successfully removed.
 - Label device with LPAA label.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **MRS**
 - o If reset failed:
 - Create Sanitization Log Record.
 - Sanitization Status Code: **MRFMD**
 - **Follow process for broken or damaged device.**
 - o If reset is not available:
 - **Follow process for broken or damaged device.**
 - For broken or damaged devices:
 - o Destroy device using approved destruction methods (see Sanitization Requirements).
 - o Create Sanitization Log Record.
 - o Sanitization Status Code: **DS**

- **Backup Tapes - (Magnetic Tape)**
 - For all:
 - o If Degausser is available:
 - Degauss
 - Create Sanitization Log Record
 - Sanitization Status Code: **DGS**
 - o If Degausser is not available:
 - Destroy tape using approved destruction methods (see Sanitization Requirements).
 - Create Sanitization Log Record.
 - Sanitization Status Code: **DS**

- **Server or Network Storage**
 - For all:
 - o Remove each individual storage drive.
 - o **Follow process for HDD**
 - o If an alternative approach is preferred:
 - Document alternative approach.
 - Send to OTS Information Security for review and approval.
 - Written approval must be obtained from OTS Information Security prior to performing any alternative procedures or solutions for sanitizing any server or network storage.

Data Sanitization – Standards and Requirements

Approved Processes (Cont.)

- **DRAM, SRAM, or NOVRAM – (RAM)**
 - For all:
 - Remove power or battery for a minimum of 5 minutes.
 - Create Sanitization Log Record.
 - Sanitization Status Code: **PRS**

- **EAPROM, EEPROM, or EPROM – (ROM)**
 - For all:
 - Destroy media using approved destruction methods (see Sanitization Requirements).
 - Create Sanitization Log Record.
 - Sanitization Status Code: **DS**

Sanitization Status Codes

To ease any review process: below is a mapping of devices or media type to potential code and includes Sanitization Method and Status translation.

Media Type	Code	Method	Status	Condition
Office Equipment	ND	N/A	No Data	Reusable
HDD, SSD	OWS	Overwrite	Success	Reusable
Facsimile, Office Equipment, Network Device, Mobile Device	MRS	Reset	Success	Reusable
RAM	PRS	Removed Power	Success	Reusable
HDD	OWFD	Overwrite	Failure – Marked for Degaussing	Not Reusable
HDD, SSD	OWFMD	Overwrite	Failure – Marked for Destruction	Not Reusable
Network Device, Mobile Device	MRFMD	Reset	Failure – Marked for Destruction	Not Reusable
Facsimile, Office Equipment, Network Device, Mobile Device, Magnetic Tape, ROM	DS	Destruction	Success	Not Reusable
HDD, SSD	OWFDS	Destruction	Success	Not Reusable
HDD, Magnetic Tape	DGS	Degaussed	Success	Not Reusable
Optical Media	OMDS	Destruction	Success	Not Reusable
Removable Media	RMDS	Destruction	Success	Not Reusable

Data Sanitization – Standards and Requirements

Related Policies, Standards, Guidelines

OTS Data Classification Policy

OTS Data Sanitization Policy

OTS Drive Overwrite SOP-101

OTS Drive Overwrite SOP-102

LPAA POL 201401

Owner

Division of Administration, Office of Technology Services

Effective Date

11/15/2014

Document ID: OTS-1001-1001-001

Revision History

Date	Author	Description
2014-10-21	Ivory Junius	Creation
2014-11-10	Dustin Glover	Revision

Appendix E – Portable Computing Device Release Form
Portable Computing Device (PCD) Release
Form
LSU HCSD Portable Computing Device Use
Agreement

As the user of a portable computing device (tablet, laptop, phone) owned/supplied by a Louisiana State University entity you agree to the following provisions:

I. Obligations

Once the term of 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. No PII, PHI, Intellectual property, or Organization Proprietary data should be stored on portable computing devices or removable storage media unless for a defined business need and proper administrative approvals have been documented. Data that is stored to the PCD should be also stored on the user's O:\ drive as soon as possible.

III. Theft

If the PCD is lost or stolen it must be reported to the agency's IT Director, Privacy Officer, and the agency police immediately. For phones the carrier should also be notified. 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. Game, entertainment software, or personal finance software should not be loaded on an LSU owned PCD computer.

VI. Virus, Hacking, and Security Protection

To ensure that virus protection and other security patches are current, PCDs must be connected to the LSU network at least on a monthly 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. Devices should not be connected to unsecure wifi.

VII. Indemnity

LSU is not responsible for any injuries, damages, claims, including legal expenses, 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.

_____	_____
Make	Model
_____	_____
Serial Number	State Property Tag

Printed Name	
_____	_____
Phone Number	Email Address
_____	_____
Date Received	Signature
_____	_____
Date Returned	Received from Signature

	Received by Signature