LOUISIANA STATE UNIVERSITY
HEALTH CARE SERVICES DIVISION

POLICY NUMBER:	7701-24
CATEGORY:	Information Security
CONTENT:	Information System and Data Security
APPLICABILITY:	This policy applies to all persons employed by the LSU Health Care Services Division (HCSD) and/or the Lallie Kemp Medical Center (LKMC) either through direct hire or through contractual arrangement.
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 Revised: November 7, 2024
INQUIRIES TO:	Information Technology LSU Health Care Services Division P.O. Box 91308 Baton Rouge, LA 70821-1308

Note: Approval signatures/titles are on the last page

LOUISIANA STATE UNIVERSITY
HEALTH CARE SERVICES DIVISION

INFORMATION SYSTEM AND DATA SECURITY

Table of Contents

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 Messaging) and LSU HCSD 4512 (Internet), LSU HCSD 0517 (Cellular Equipment and Wireless Devices, LSUHSC-NO CM 42 (Information Technology Infrastructure), LSUHSC-NO EIS 100 (LSUHSC New Orleans Enterprise Information Security Policy), and the regulations of the Louisiana Office of InformationTechnology.

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 Section I, 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.

Information Security and Data Security is specific to the operations of LSU HCSD and is derived in part from PM-36 and EIS-100.

III. DEFIITIONS

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. Owner

Person or entity with fiduciary responsibility for an asset; should understand the responsibility of maintaining the security of the asset and have approved management responsibility for controlling the whole lifecycle of an asset; should be able to help define the value of the asset; must evaluate the asset to be assured that the asset receives the appropriate level of security.

F. Custodian

Person or group responsible for safekeeping an IT asset or property on behalf of the Owner. Custodian can be the IT Department responsible for managing the equipment and systems on which the IT asset is contained. Custodian can also be the person responsible for their assigned IT Asset, such as workstations and mobile devices.

IV. IMPLEMENTATION

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

V. ENFORCEMENT/VIOLATIONS

Failure to adhere to the intent of this policy may result in disciplinary action up to and including dismissal.

VI. EXCEPTIONS

The HCSD CEO or designee may waive, suspend, change, or otherwise deviate from any provision of this policy they deem necessary to meet the needs of the agency as long as it does not violate the intent of this policy; state and/or federal laws; Civil Service Rules and Regulations; LSU Policies/Memoranda; or any other governing body regulations.

VII. POLICY AND PROCEDURE STATEMENTS

The HCSD Information Security Policy / Procedure statements below are to clarify HCSD's implementation of LSU Permanent Memorandum 36 (PM36).

Chapter 1 – Securing Systems, Hardware, Software and Peripherals

Subunit 1 – Purchasing and Installing Hardware

Policy Statement 1.1.1 – Security Standards and Guidelines

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, to ensure the confidentiality, integrity, and availability of the data stored on its information systems:

1. LSU HCSD 7521 (HIPAA Administrative, Technical and Physical Safeguards)
2. LSU HCSD 4511 (Email and Messaging)
3. LSU HCSD 4512 (Internet)
4. LSU HCSD 0517 (Cellular Equipment and Wireless Device)
5. LSU HCSD 4565 (IT Violations and Disciplinary Actions)
6. LSU HCSD 4570 (Telework)
7. The LSUHSC-NO Enterprise Information Security (EIS) 100
8. LSUHSC-NO CM 42 (Information Technology Infrastructure)
9. Any additional information security standards set at an LSU HCSD facility that are more restrictive than the above

This policy shall be reviewed periodically and updated as necessary.

Policy Statement 1.1.2 Specifying Information Security Requirements for New Systems

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 LSUHSC-NO 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 LSUHSC-NO Enterprise Information Security (EIS), LSU HCSD has adopted the LSUHSC-NO EIS workstation and server standards, see Appendix A – Workstation and Server Standards, and the LSU HCSD application security guidelines, reach out to your facility IT department for a copy of these 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.

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

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

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 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

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

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. When not establishing a recurring encrypted file transfer process, LSU HCSD has available to staff the use of the LSU Secure File Transfer Systems, LSU Files, which should be utilized as the preferred method to transmit protected or restricted 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

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.

Documents containing protected or restricted information shall never be printed at a public location, such as a hotel business center, a printing center like Kinkos, or any other public printing location.

Documents containing protected or restricted information should never be printed at home or other private location not affiliated with LSU HCSD, unless remote work has been authorized.

Policy Statement 1.2.6 Securing Network Cabling

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 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. If supported by the system, any removable media used to store protected or restricted information must be encrypted. Any removable media used to store protected or restricted information shall be issued and logged by the IT Department and must be returned to the IT Department, after use, for proper disposal. 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 removing protected or restricted information from 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 in accordance with the following points:

1. Appropriate administrative approval has been secured.
2. If the information is digital, it is contained on encrypted removable media issued by the IT Department.
3. All information is kept securely concealed and inaccessible to others by physical means.
4. Only the employee has knowledge of or access to the information while off campus.
5. Only the minimum information necessary to accomplish the task is removed from campus.
6. Removable media used is returned to the IT Department upon completion of the defined business need.

Subunit 4 – Working Off Campus or Using Outsourced Processing

Policy Statement 1.4.1 – Contracting or Using Outsourced Processing

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.

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

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 the 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.

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 shutdown and stored out-of-sight when the employee must leave the device at the hotel. 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 local law enforcement and a police report obtained.

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 for ensuring 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 Remotely

LSU HCSD employees working from off campus locations shall adhere to LSU HCSD Telework Policy, 4570. 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 HCSD systems or information shall require an encrypted connection to the LSU HCSD Network to ensure against unauthorized interception and/or disclosure of information.

Policy Statement 1.4.4 – Use of Personal Computing Devices

LSU HCSD employees using personally owned computing devices for LSU HCSD business must follow LSU HCSD Cellular Equipment and Mobile Device Policy, 0517. LSU HCSD employees must understand and follow the acceptable use of a personal computing device as detailed in LSU HCSD Policy 0517, LSUHSC-NO CM-42 and LSUHSC-NO EIS-100, while the device is connected to the LSU HCSD network infrastructure. LSU HCSD employees must ensure any personal computing device used for LSU HCSD business or connected to LSU HCSD network infrastructure meet all requirements for protecting and securing the device, as detailed in LSU HCSD Policy 0517 and LSUHSC-NO EIS-100, including, but not limited to, encryption of the LSU HCSD data on the device, maintaining current operating system patches, and maintaining current antivirus and antimalware software patches. Guidelines for securing a personal computing devices are outlined in LSU HCSD Cellular Equipment and Mobile Device Policy, 0517. LSU HCSD data and systems access from personal computing devices are, at all times, the property of LSU HCSD. LSU HCSD employees must allow LSU HCSD IT and Compliance staff access to any personal computing device used to access LSU HCSD data, for the purpose of security and compliance investigations.

Subunit 5 – Encryption

Policy Statement 1.5.1 – Encryption

LSU HCSD shall follow the encryption requirements set forth in LSUHSC-NO CM-42 and LSUHSC-NO EIS-100. LSU HCSD shall document encryption standards for encryption of data at rest and encryption of data in motion. Any data stored on LSU HCSD servers, workstations and mobile devices shall be encrypted or compensating controls must be in place to protect this data. All data backup systems shall have encryption enforced. All websites, internal and external facing, shall enforce encryption of data during transmission, using SSL encryption. All wireless network connections to the internal LSU HCSD network shall have encryption enforced. Portable computing devices must also adhere to the LSU HCSD Cellular Equipment and Wireless Devices Policy, 0517.

Policy Statement 1.5.2 – Management of Encryption Keys

LSU HCSD shall have a written procedure to manage encryption keys related to requesting, verifying, approving, installing, and revoking encryption keys, where a formal process is appropriate. For example, website certificate management should be documented in this procedure.

Policy Statement 1.5.3 – Storage of Encryption Keys and Secrets

LSU HCSD shall use a secure vault for secure storage of all encryption certificate keys, for website and database encryption. LSU HCSD shall use this secure vault for storage of all critical passwords and secrets.

Subunit 6 – Hardware and System Documentation

Policy Statement 1.6.1 – Maintaining and Using Hardware and System Documentation

Up to date hardware and system documentation, such as operator manuals or technical information provided by suppliers or vendors, shall be readily available to staff who are authorized to support or maintain the system.

Subunit 7 – Other Hardware Issues

Policy Statement 1.7.1 – Destruction and/or Reuse of Equipment

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. 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 1.7.2 – Recording, Reporting, and Correcting System Faults

Note: This section is written with the clear understanding that the LSU HCSD network is an integral part of the LSUHSC-NO network. Due to this relationship, many procedures include use of the LSUHSC-NO 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 LSUHSC-NO 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 LSUHSC-NO Department of Information Technology staff, the Enterprise Information Security Manager or designee shall immediately notify the HIRT via the email distribution list. The LSUHSC-NO Enterprise Information Security Manager will determine if activation of the LSUHSC-NO 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. LSUHSC-NO Enterprise Information Security Manager
vi. Other personnel as deemed appropriate

CSIRT Membership

i. LSUHSC-NO Enterprise Information Security Manager (Chair)
ii. LSUHSC-NO 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 LSUHSC-NO IT resources without authorization.
ii. Denial of Service – An individual or group coordinates Internet traffic directed at LSUHSC-NO 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 LSUHSC-NO or personally owned, on LSUHSC-NO premises or via the LSUHSC-NO 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 LSUHSC-NO 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 1.7.3 – Logon and Logoff from Computer

Logon/ Logoff procedures shall be strictly followed. No person given access privileges to the LSU HCSD 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 1.7.4 Damage to Equipment

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 in accordance with HCSD Policy 2538.

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

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

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 HSCD 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

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.

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

External Affiliate – External Affiliates are users who require access to LSU HCSD computer resources, but are not LSU HSCD 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:

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

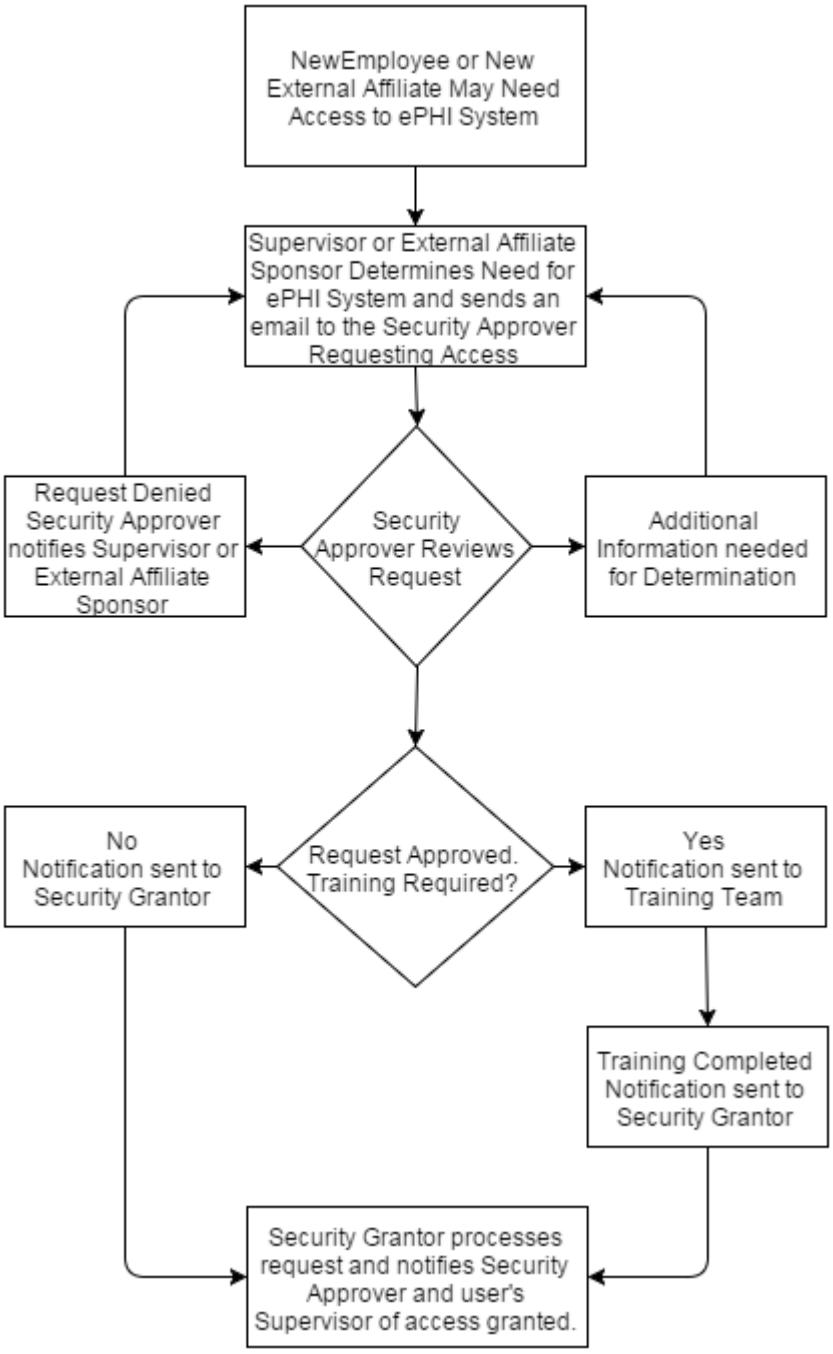
Each LSU HCSD facility and External Affiliate sponsor will designate a process whereby employees

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.


NewEmployee or New External Affiliate May Need Access to ePHI System
Supervisor or External Affiliate Sponsor Determines Need for ePHI System and sends an email to the Security Approver Requesting Access
Request Denied Security Approver notifies Supervisor or External Affiliate Sponsor
Security Approver Reviews Request
Additional Information needed for Determination
No Notification sent to Security Grantor
Request Approved. Training Required?
Yes Notification sent to Training Team
Training Completed Notification sent to Security Grantor
Security Grantor processes request and notifies Security Approver and user's Supervisor of access granted.

Use of Generic IDs (Service Accounts)

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 LSUHSC-NO 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 LSUHSC-NO standards and methods for generic ID as outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Enterprise Computer Services.

Policy Statement 2.1.3 – Securing Unattended Workstations

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 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 LSUHSC-NO standard for network access controls outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Enterprise Computer Services.

Policy Statement 2.1.5 Managing Application Access Control

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 LSU HCSD CIO.

Policy Statement 2.1.6 Managing Passwords

LSU HCSD has adopted the LSUHSC-NO standard for password length, password change interval, password complexity outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Enterprise Computer Services. The LSUHSC-NO password standard will be implemented in applications that are capable of supporting the standard. See LSUHSC-NO EIS 100 Appendix B for specific password requirements.

Policy Statement 2.1.7 Unauthorized Physical Access Security

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

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 a 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, as outlined in the above Policy Statement 1.7.2 - Recording, Reporting, and Correcting System Faults.

Policy Statement 2.1.9 Managing System Access

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 LSUHSC-NO 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

Remote user access to LSU HCSD information and systems is controlled via the standards and methods outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Department of Information Technology. These methods ensure accurate authentication of remote users, and the integrity and confidentiality of the information transmitted. The acceptable methods for accessing the LSU Health System Network remotely shall utilize a virtual private network (VPN), and/or Citrix

Netscaler Connection.

Policy Statement 2.1.11 – Emergency Access

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 or unavailable employee is again available, access to the system will be granted according to the following procedure. 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 LSUHSC-NO 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

LSU HCSD has adopted the LSUHSC-NO 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 LSUHSC-NO Department of Information Technology.

Policy Statement 3.1.2 Managing the Network

Personnel responsible for managing the LSUHSC-NO Network and preserving its integrity in support of LSU HCSD shall do so in accordance with the standards and methods outlined in LSUHSC-NO EIS 100. LSU HCSD has adopted these LSUHSC-NO standards to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Department of Information Technology.

Policy Statement 3.1.3 Defending Network Information against Malicious Attack

LSU HCSD has adopted the standards outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by

LSUHSC-NO Department of Information Technology. LSU HCSD ensures, where systems are capable, that all workstations and servers are running malware protection software and are running endpoint protection software. If systems are not capable of running this software, compensating controls are implemented.

Subunit 2 System Operations and Administration

Policy Statement 3.2.1 Appointing System Administrators

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 LSUHSC-NO personnel, system administrators shall be appointed according to applicable LSUHSC-NO 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

LSU HCSD employees and affiliates shall be granted access to data based on the Minimum Necessary standard. Each LSU HSCD 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.

LSU HCSD employees shall use appropriate methods to share data internally. Protected or restricted data shall only be shared using secure data sharing methods. Acceptable methods include file shares on internal file servers; LSU HCSD licensed and approved cloud services - such as the LSU HCSD licensed Microsoft 365 (OneDrive, Teams and SharePoint) tenant; Microsoft Azure cloud services; LSUHSC-NO secure file sharing solution LSU Health FileS; and the Epic Electronic Health Record. The local IT Department can provide a full list of acceptable file sharing methods.

LSU HCSD employees shall refer to the LSU HCSD Email and Messaging Policy, 4511, regarding proper use of and data sharing of protected and restricted data through email.

Policy Statement 3.2.3 – Permitting Third Party Access

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 agreements. 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.

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 LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Department of Information Technology.

LSU HCSD employees shall use appropriate tools to share data externally. Protected or restricted data shall only be shared using secure data sharing methods. Acceptable methods include file shares on internal file servers, if the external party has been issued LSU HCSD credentials; LSU HCSD licensed and approved cloud services - such as the LSU HCSD licensed Microsoft 365 (Teams and SharePoint) tenant, but only after creating the appropriate structure through the local IT Department; Microsoft Azure cloud services, but only after creating the appropriate structure through the local IT Department; LSUHSC-NO secure file sharing solution LSU Health FileS; and the Epic Electronic Health Record, if the external party has been issued Epic EHR credentials. The local IT Department can provide a full list of acceptable file sharing methods.

LSU HCSD employees shall refer to the LSU HCSD Email Policy, 4511, regarding proper use of and data sharing of protected and restricted data through email.

Policy Statement 3.2.4 – Ensuring Information Integrity

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.

Subunit 3 – E-mail and the Internet

Policy Statement 3.3.1 – Downloading Files and Information From the Internet

LSU HCSD has adopted the LSUHSC-NO 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 LSUHSC-NO Department of Information Technology. All faculty, staff, students, employees, vendors, and external affiliates shall abide by LSUHSC-NO CM-42 and HCSD Internet policy 4512. CM-42 and LSU HCSD Internet Policy, 4512, provide guidelines to ensure information, software, and media downloaded from the Internet does not jeopardize the operations, reputation, or security of the LSUHSC-NO and LSU HCSD network.

Policy Statement 3.3.2 – Sending and Receiving Electronic Mail (E-Mail) and/or Other Forms of Digital Communication

LSU HCSD has adopted the LSUHSC-NO standards and methods for digital communications generated by LSU HCSD information systems outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Department of Information Technology. All inbound and outbound external and internal email shall be scanned for viruses by the email system. In addition to the basis provided by EIS 100, LSU HCSD email communications are defined by the additional standards and

methods outlined in the LSU HCSD Email and Messaging Policy 4511, which prohibits any transmission of PHI via email.

Subunit 4 – Data Management

Policy Statement 3.4.1 – Transferring and Exchanging Data

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 and encrypted method of transfer approved by LSUHSC-NO 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. Use of removable media to support the transfer of information must comply with Policy Statement 1.3.1 – Using Removable Storage Media Including Diskettes and CDs.

Policy Statement 3.4.2 – Managing Data Storage

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 the integrity and confidentiality of 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 and must comply with Policy Statement 1.3.1 - Using Removable Storage Media Including Diskettes and CDs.

Subunit 5 – Backup, Recovery, and Archiving

Policy Statement 3.5.1 – Transferring and Exchanging Data

LSU HCSD Policy / Procedure
All LSU HCSD information systems containing protected or restricted information shall be protected by adequate backup and system recovery procedures. These backups shall be encrypted. 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 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 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

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 system's 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 necessary. 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 B.

Chapter 5 – Developing and Maintaining Custom Software

Subunit 1 – Controlling Software Code

Policy Statement 5.1.1 – Managing Operational Program Libraries

All operational program libraries for critical applications developed by LSU HCSD shall reside in the LSU HCSD code library. Access to operational program libraries shall be controlled through security roles within the code library.

Policy Statement 5.1.2 – Managing Program Source Libraries

All program source libraries, executables, and linked libraries for critical applications developed by LSU HCSD shall reside in the LSU HCSD code library. Access to operational program libraries shall be controlled through security roles within the code library.

Policy Statement 5.1.3 – Controlling Deployment of Software Code During Software Development

All changes to LSU HCSD source libraries and operational program libraries shall be properly authorized and tested before moving to the production environment.

Subunit 2 – Software Development

Policy Statement 5.2.1 – Software Development

LSU HCSD has adopted the LSUHSC-NO Application Security Standards outlined in LSUHSC-NO EIS 100 to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Department of Information Technology. All new applications shall adhere to the Application Security Guidelines.

Subunit 3 – Testing and Training Environments

Policy Statement 5.3.1 – The Use of Protected Data for Testing

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

System owners will work with the facility IT Directors, application vendors/developers, HR, 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 – Business Continuity Planning

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

Policy Statement 6.1.1 Initiating the BCP/DRP

LSU HCSD shall develop, implement and maintain a written IT Business Continuity Plan (BCP)/ Disaster Recovery Plan (DRP) to ensure the continuation of key information systems services in the event these services are disrupted. LSU HCSD is responsible for annually reviewing and updating this plan.

Policy Statement 6.1.2 Assessing the BCP/DRP Security Risk

LSU HCSD shall conduct ana annual criticality rating in order to determine the requirements for the BCP/DRP.

Policy Statement 6.1.3 Testing the BCP/DRP

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 CIO. The BCP/DRP shall be produced in the appropriate format to guarantee its availability during an emergency.

Policy Statement 6.1.4 Training and Staff Awareness of the BCP/DRP

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

Chapter 7 – Addressing Personnel Issues Relating to Security

Subunit 1 Contractual Documentation

Policy Statement 7.1.1 Preparing Conditions of Employment

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.

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 LSUHSC-NO 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 HCSD information, all access shall be terminated immediately.

All new LSU HCSD employees, faculty, staff, and students shall receive Information Security training appropriate for their job function. Each new user shall complete the initial LSU HCSD 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 7.1.2 Employing/Contracting New Staff

See LSUHSC-NO CM 42 LSU HCSD Policies 7500, 8501, 4515, 4547, 4546, 4522, 4538, and 4539.

Policy Statement 7.1.3 External Suppliers/Other Vendor Contracts

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 7.1.4 Non-Disclosure Agreements

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. LSU HCSD maintains a Business Associate Agreement (BAA) template for consistent implementation.

Subunit 2 – Personnel Information Security Responsibilities

Policy Statement 7.2.1 Passwords and PIN Numbers

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 1.7.3 – Logon and Logoff from Computer

Subunit 3 – Employment Termination

Policy Statement 7.3.1 – Staff Resignations

LSU HCSD has adopted the LSUHSC-NO procedure for revoking access to LSU HCSD/ LSUHSC-NO information systems to support consistency and compliance with the network and application security infrastructure managed for LSU HCSD by LSUHSC-NO Office of Computer Services.

Routine separations will be managed through the automated process developed by LSUHSC-NO EIS using the Identity Access Management system of LSUHSC-NO.

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

Policy Statement 7.3.2 – Procedures for Staff Leaving Employment

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

Chapter 8 – Training and Staff Awareness

Subunit 1 Training and Awareness

Policy Statement 8.1.1 Information Security Training and Awareness

LSU HCSD Compliance, HIPAA Privacy and HIPAA Security training modules have been developed to be presented to employees of LSU HCSD at General Orientation, Contracted Employee Orientation, and Medical Staff/Resident Orientation. In cases where workforce members do not have computer access, actual hard copies of the policies will be provided. These methods will have an attestation the employee/resident received the material.

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.

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 that the Compliance Officer/Privacy Officer or Security Officer must be notified if these policies are not followed.

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 each individual's supervisor is responsible to ensure this training is completed.

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.

Policy Statement 8.1.2 Anti-Phishing Campaign

LSU HCSD shall maintain an anti-phishing campaign designed to train and educate employees about phishing. This campaign will include annual mandatory education material specific to phishing. This campaign will include testing the ability of employees to recognize and report phishing emails by sending test phishing emails. These tests will be monitored, and results reported to the LSU HCSD HIPAA Security Committee, on a per campaign basis, where appropriate

additional training and education will be provided. The annual results of the anti-phishing campaign will be reported to the LSU HCSD Executive Staff.

Chapter 9 – Physical Security

Subunit 1 Campus Security

Policy Statement 9.1.1 Preparing Campus for Placement of Computers

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 10 – Information Security Incidents

Subunit 1 Reporting Information Security Incidents

Policy Statement 10.1.1 Defending Against Unauthorized or Criminal Activity

LSU HCSD has adopted the LSUHSC-NO 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 LSUHSC-NO Department of Information Technology. LSU HCSD shall maintain an Information Security Incident Response Plan.

Policy Statement 10.1.2 Security Incident Procedures

LSU HCSD shall adhere to the LSUHSC-NO EIS and LSU HCSD Incident Response Procedure, as defined above in Policy Statement 1.7.2 - Recording, Reporting, and Correcting System Faults.

Subunit 2 Investigating Information Security Incidents

Policy Statement 10.2.1 Investigating the Cause and Impact of Information Security Incidents

LSU HCSD shall adhere to the LSUHSC-NO EIS and LSU HCSD Incident Response Procedure, as defined above in Policy Statement 1.7.2 - Recording, Reporting, and Correcting System Faults. 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 10.2.2 Responding to Information Security Incidents

LSU HCSD shall adhere to the LSUHSC-NO EIS and LSU HCSD Incident Response Procedure, as defined above in Policy Statement 1.7.2 - Recording, Reporting, and Correcting System Faults. 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 11 – Classifying Information and Data

Subunit 1 Setting Classification Standards

Policy Statement 11.1.1 Defining Information

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

Policy Statement 11.1.2 Classifying Information

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 11.1.3 Characteristics and Handling of Protected 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.

Policy Statement 11.1.4 Characteristics and Handling of Restricted Information

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 – Appendix A

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 LSU Health Sciences Center - New Orleans (LSUHSC-NO) network. This document does not provide the information necessary to correctly administer a workstation or server. It is assumed that the IT staff 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. Any exceptions must be approved and documented.

A.1 Workstation Standards

All workstations connected to the LSUHSC-NO network shall be configured according to the following guidelines:

1. Workstations shall be configured to receive patches via an automated patching system such as Intune or SCCM.
2. The institutional standard OS version shall be properly installed and configured and all relevant security patches for both the OS and all necessary applications shall be applied.
3. Workstations shall be configured to synchronize internal system clocks to an LSUHSC-NO-approved authoritative time source.
4. 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.
5. All services running on a workstation shall be patched and secured properly before being enabled.
6. No workstations are allowed to run DNS or DHCP server services under any circumstances.
7. All default passwords shall be changed immediately and shall be in accordance with LSUHSC-NO password policy. Passwords shall not be stored unencrypted.
8. Administrator access shall be limited to the smallest number of people necessary to properly maintain workstations and allow access in case of emergencies.
9. 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.
10. The institutional Endpoint Detection and Response (EDR) shall be properly installed, configured, and updated.
11. Every workstation shall use a dynamically assigned IP address. If the workstation requires a static IP address, the computer supporter shall consult with LSUHSC-NO Department of Information Technology (DIT) to establish the requirements.
12. 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.
13. All workstations shall have access logging enabled.

A.2 Server Standards

All servers connected to the LSUHSC-NO network shall be configured according to the following guidelines:

1. Servers shall be configured to receive patches via an automated patching system such as SCCM.
2. The OS shall be properly installed and configured, and all relevant security patches for both the OS and all installed applications shall been applied.
3. Servers shall be configured to synchronize internal system clocks to an LSUHSC-NO-approved

authoritative time source.
4. 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.
5. No servers are allowed to run LDAP, DNS, DHCP, or Windows Directory Services without prior coordination with LSUHSC-NO DIT.
6. Servers shall be located in designated server rooms or secured locations.
7. All default passwords shall be changed immediately and shall be in accordance with LSUHSC-NO password policy. Passwords shall not be stored unencrypted.
8. 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.
9. Server administrators shall supply accurate contact information to LSUHSC-NO DIT for emergencies such as power outages and server break-ins. This information shall also include a general description of the server, its purpose, and any special requirements or configuration.
10. The institutional Endpoint Detection and Response (EDR) shall be properly installed, configured, and updated whenever supported by the OS.
11. Every server shall be plugged in to an Uninterruptible Power Supply (UPS).
12. Every server shall have an appropriate name, reserved IP address, and DNS record.
13. All servers shall be administered by qualified personnel.
14. 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.
15. 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 LSUHSC-NO network shall be configured according to the following guidelines:
1. Owners of equipment managed by vendors shall consult with LSUHSC-NO 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-LSUHSC-NO 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 LSUHSC-NO guidelines.
4. LSUHSC-NO 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.
6. Remote access is available via the VPN and use of Remote Desktop or SSH depending on the operating system. Unless appropriate compensating controls have been implemented in coordination with Information Security, systems connected to the LSUHSC-NO network infrastructure shall not run remote control software that maintains a connection to a cloud or vendor system thus bypassing the LSUHSC-NO firewall.

Appendix B – 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.

Document Metadata

Document Name:	7701-24- Information Security Policy.docx
Policy Number:	7701
Original Location:	/LSU Health/HCSD/7700 - Information Security
Created on:	04/26/2005
Published on:	12/16/2024
Last Review on:	12/13/2024
Next Review on:	12/13/2025
Effective on:	07/29/2019
Creator:	Kees, James "Mickey" *HCSD Chief Information Officer*
Committee / Policy Team:	Main Policy Team
Owner/SME:	Kees, James "Mickey" *HCSD Chief Information Officer*
Manager:	Kees, James "Mickey" *HCSD Chief Information Officer*
Author(s):	Wicker, Claire M. *PROJECT COORDINATOR*
Approver(s):	Wilbright, Wayne *Chief Medical Informatics Officer* Kees, James "Mickey" *HCSD Chief Information Officer*
Publisher:	Wicker, Claire M. *PROJECT COORDINATOR*

Digital Signatures:

Currently Signed

Approver:
Kees, James "Mickey"
HCSD Chief Information Officer

12/16/2024

Approver:
Wilbright, Wayne
Chief Medical Informatics Officer

12/16/2024