LSU Health New Orleans EIS 100

LSU Health New Orleans
Enterprise Information Security

Scope

This policy applies to any device that connects to the LSU Health New Orleans (LSUHNO) IT infrastructure and any person using LSUHNO IT resources. This policy is meant to augment any existing policies, laws, or regulations that currently refer to computing and network services.

Purpose

The purpose of this policy is to provide guidelines to protect the confidentiality, integrity, and availability of LSUHNO information systems.

Policy

100.1 Purchasing and Installing Information Systems

100.1.1 Security Standards and Guidelines

LSUHNO has developed technical standards to ensure the confidentiality, integrity, and availability of its information systems. All equipment and software purchased or developed shall adhere to these standards. These standards shall be reviewed no less frequently than every 3 years and shall be revised if necessary to ensure adherence to LSU University Administration Permanent Memoranda 36 (PM-36). All standards documents shall include a version number and a date of adoption for audit purposes. Systems that were installed prior to the implementation of these standards may be grandfathered until a replacement or update can be planned and implemented.

100.1.2 Specifying Information Security Requirements for New Systems All proposed information systems to be purchased with LSUHNO funds (including donations, grants, etc.) shall be submitted to the Department of Information Technology (DIT) for approval and review to ensure adherence to Enterprise Information Security standards. The DIT may, at its own discretion, set monetary and/or functional parameters to determine appropriate levels of review and/or develop and publish a pre-approved list of items which are commonly purchased.

100.1.3 Specifying Information Security Requirements for New Systems

All hardware and software installations at LSUHNO shall be planned, and parties affected by the installation shall be 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 put into the production environment. The extent of planning

and testing shall be commensurate with the size and complexity of the installation to ensure a successful implementation with a minimal disruption of operation.

100.2 IT Peripherals

100.2.1 Supplying Continuous Power to Critical Equipment

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

100.2.2 Managing High Availability Systems

The LSUHNO DIT shall identify systems managed by DIT that require a high degree of availability and shall ensure their continued operation during power failures, system faults, and other operational disruptions.

100.2.3 Using Fax Machines/Fax Modems

Protected and/or restricted information shall only be faxed when more secure methods are not available. The sender of the protected or restricted information and the intended recipient shall agree to the fax transmittal prior to sending.

100.2.4 Using Modems/ISDN/DSL/Cable Connections

In the event that protected or restricted information cannot be sent via the LSUHNO 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. Enterprise Network Support (ENS) and Enterprise Information Security (EIS) shall be consulted prior to installing any such connection on any network managed by the LSUHNO DIT.

100.2.5 Using Shared 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 the information during and after printing.

100.2.6 Securing Network Cabling

All cabling in LSUHNO networks shall be secured to prevent damage or unauthorized interception of data. To prevent abuse of network facilities, all network connections shall be monitored or secured by ENS.

100.2.7 Securing Removable Storage Media

All protected or restricted information stored on removable media, shall be kept in a safe, secure environment in accordance with the manufacturers' specifications when not in use. All methods available shall be used to secure removable media when removed from the LSUHNO premises.

100.3 Working Off Campus or Using Outsourced Processing

100.3.1 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 LSUHNO Business Associate Agreement and LSUHNO EIS standards.

100.3.2 Use of Laptop/Portable Computers, Portable Electronic Devices, and the Removal of Equipment from LSUHNO

Laptops and/or other portable computing devices issued to LSUHNO employees shall not be used for activities unrelated to LSUHNO organizational goals. Computer supporters shall document who is in possession of each device and that the user understands their responsibility for the confidentiality, integrity, and availability of information on said device. Each LSUHNO employee, who is assigned a mobile computing device, shall be responsible for ensuring that the operating system is patched in a timely fashion, that access to the device is protected by a password, and where applicable anti-virus software with a current virus data file is installed and running continuously, and the device, if supported, is encrypted. Only authorized personnel shall be permitted to take any equipment belonging to LSUHNO off the premises and are responsible for securing the assigned equipment at all times.

100.3.3 Remote Access to Network Resources

LSUHNO users shall utilize a VPN and/or Citrix connection to the LSUHNO network to ensure the confidentiality, integrity, and availability of protected data accessed during any remote access session.

100.4 Hardware and System Documentation

100.4.1 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.

100.5 Other Hardware Issues

100.5.1 Destruction and/or Reuse of Equipment

IT equipment and/or media owned by LSUHNO shall only be disposed of by authorized personnel in accordance with Louisiana Property Assistance Agency (LPAA) policies and procedures. In addition, LSUHNO internal policies for data sanitization require that the serial numbers of all hard drives wiped or shredded must be recorded and retained, and any tool used to wipe a drive must also verify that the wipe was successful. IT equipment and/or media owned by LSUHNO which is reused shall be evaluated as to whether protected or restricted information needs to be purged in accordance with the above standards prior to reuse or disposal.

100.5.2 Recording, Reporting, and Correcting System Faults

The LSUHNO Disaster Recovery Plan (DRP) shall be used as guidance for documenting and responding to significant information system incidents that impact multiple users.

100.5.3 Damage or Theft of Equipment

All deliberate damage to or theft of LSUHNO IT property or personally owned devices that contain LSUHNO data shall be reported to the Compliance Office or Campus Police as soon as it is discovered.

100.6 Controlling Access to Information and Systems

100.6.1 Managing Access Control

All access to LSUHNO information systems shall be based on the principle of least privilege.

100.6.2 Managing User Access

Access to the LSUHNO information systems is granted to anyone actively affiliated with the university. Each faculty, staff, student, and external user shall be assigned a unique user ID. When generic IDs are required by operational necessity, the generic account policies (Appendix B) must be followed to prevent abuse. EIS will maintain records of resource authorization for six years after access is terminated.

100.6.3 Passwords and PIN Numbers

All LSUHNO faculty, staff, students, and external users shall secure passwords, PINs, and other methods of authentication as private and highly confidential.

100.6.4 Information Security Training

All LSUHNO users shall complete information security training commensurate with their duties and responsibilities. Training requirements shall be reassessed when duties or responsibilities change.

100.6.5 Securing Unattended IT Equipment

Precautions shall be taken to prevent tampering of unattended equipment. All information systems storing protected or restricted information shall incorporate technical methods to secure unattended workstations in unsecured areas to prevent unauthorized use.

100.6.6 Managing Administrative Access

Administrative access to applications, operating systems, and supporting infrastructure shall require authorization from the employee's supervisor and/or the owner of the resource.

Administrative access shall be restricted to those persons who are authorized and are responsible for administration/management functions.

100.6.7 Managing Passwords

All LSUHNO computer accounts must be password protected in accordance with the LSUHNO password policy (Appendix B).

100.6.8 Physical Access

Physical access to areas housing or supporting IT infrastructure shall be protected using all reasonable and appropriate safeguards.

100.6.9 Monitoring System Access and Use

All LSUHNO information systems that contain protected or restricted information shall be configured to log any and all information necessary to detect and record attempts of unauthorized access and system errors, to the extent that the logging facility exists and is capable.

100.6.10 Defining and Classifying Information

All LSUHNO departments shall adopt a method to classify information assets that includes ranking each asset with regards to confidentiality, integrity, availability, and criticality to operations. The selected method shall not be less restrictive than the method defined by Louisiana state law.

100.6.11 Managing System Access

Access controls for information systems shall be set in accordance to the value and classification of the information assets being protected.

100.6.12 Controlling Remote User Access

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.

100.6.13 Emergency Access

Granting emergency access to electronic information by a user who would not normally have access to such information shall be managed and documented by EIS.

100.7 Networks

100.7.1 Configuring Networks

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

100.7.2 Managing the Network

Those responsible for managing the LSUHNO network and preserving its integrity shall do so in accordance with the DIT standards and job descriptions.

100.7.3 Defending Against Malicious Attack

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.)

100.8 System Operations and Administration

100.8.1 Appointing System Administrators

The DIT shall appoint system administrators who demonstrate the qualifications established by the department to manage the information technology systems and oversee the day to day security of these systems. Only qualified staff or contracted vendors shall repair information system hardware faults.

100.8.2 Controlling Data Distribution

When 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 prevented by using all available technical controls.

100.8.3 Permitting Third Party Access

Third party access granted to LSUHNO information systems that contain protected or restricted information shall be documented by a Business Associate Agreement and/or External Affiliate Policies (Appendix B) that specify the access to be granted and the controls to be used by both parties to ensure confidentiality, integrity and availability of the data. All third party user accounts shall validated no more than 120 days from the date access was originally granted or access was last validated.

100.8.4 Ensuring Information Integrity

LSUHNO shall implement the appropriate procedures within the Disaster Recovery Plan (DRP) to ensure that the integrity of protected or restricted information is maintained in the event of processing errors, system failures, human errors, natural disasters, and deliberate acts.

100.9 E-Mail and the Internet

100.9.1 Downloading Files and Information From the Internet

Faculty, staff, students, and external users shall abide by CM-42, which provides guidelines to ensure Internet downloads do not jeopardize the operations, reputation, or security of the LSUHNO network.

100.9.2 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.

100.9.3 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.

100.9.4 Website Maintenance

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.

100.10 Data Management

100.10.1 Transferring and Exchanging Data

All restricted or protected information shall be transferred or copied to other media only when the confidentiality and integrity of the data can be assured.

100.10.2 Managing Data Storage

All data stored on LSUHNO information systems shall be managed in a way to ensure the confidentiality, integrity, and availability of the data.

100.10.3 Backup and Recovery

All essential LSUHNO information systems shall be protected by adequate backup and system recovery procedures. The LSUHNO DRP shall be used as guidance for backups to ensure the integrity of data files.

100.11 Software Purchasing, Maintenance, and Upgrade

100.11.1 Using Licensed Software

All terms and conditions of software license agreements shall be strictly adhered to in order to comply with applicable laws.

100.11.2 Supporting Application Software

All LSUHNO software shall be maintained to ensure that business operations are not compromised. Every effort shall be made to resolve software problems efficiently and within an acceptable time period.

100.11.3 Disposing of Information Systems Software

Disposal of information systems software shall not occur unless the information systems software is no longer required and/or its related data can be archived and will not require restoration in the future.

100.12 Controlling Software Code

100.12.1 Managing Operational Program Libraries

All operational program libraries for critical applications developed by LSUHNO shall reside on enterprise servers. Access to

operational program libraries shall be controlled by EIS and provided on an as needed basis.

100.12.2 Managing Source Program Libraries

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.

100.12.3 Controlling Deployment of Software Code

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

100.12.4 Software Development

Software developed by LSUHNO for systems identified as critical to campus operations must always follow software development best practices.

100.13 Testing and Training Environments

100.13.1 The Use of Protected Data for Testing

The use of protected or restricted data in a test environment shall be adequately controlled. Access to test environments shall be granted as needed.

100.13.2 New System Training

LSUHNO users and technical staff shall be trained in the functionality and operations of all new systems to which they have access. System owners shall determine who is responsible for the appropriate systems training.

100.14 Complying with Legal Obligations

100.14.1 Awareness of Legal Obligations

All LSUHNO faculty, staff, students, and external users shall be informed of their legal responsibilities in relation to the use of computer based information and data.

100.14.2 Copyright Compliance

All LSUHNO faculty, staff, and students shall be informed of their obligation to comply with applicable copyright laws.

100.14.3 Computer Misuse: Legal Safeguards

All LSUHNO faculty, staff, and students shall be informed of changes to new and existing federal or state laws governing the use of IT devices and infrastructure.

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

100.15.1 Initiating the BCP/DRP

Each LSUHNO department shall follow procedures within the LSUHNO DRP to ensure the continuation of key information services in the event that IT services are disrupted. DRPs shall be reviewed no less frequently than every three years and shall be revised if necessary to ensure new systems are integrated into the recovery procedures.

100.15.2 Assessing the BCP/DRP Security Risk

A formal risk assessment shall be conducted in order to determine requirements for LSUHNO DRPs. Each LSUHNO department shall review its risk assessment after each emergency and at least every three years.

100.15.3 Testing the BCP/DRP

Each LSUHNO department shall test the BCP/DRP at least annually and follow the appropriate procedures regarding testing. The BCP/DRP shall be produced in the appropriate format to guarantee its availability during an emergency.

100.15.4 Training and Staff Awareness of the BCP/DRP

All appropriate LSUHNO staff shall be periodically informed of their respective roles in the BCP/DRP.

100.16 Contractual Documentation

100.16.1 Conditions of Employment

All LSUHNO employees shall acknowledge compliance with Enterprise Information Security policies as applicable to job duties.

100.16.2 Employing/Contracting Staff

LSUHNO shall verify that employees and contractors are eligible to participate in LSUHNO business and its affiliated programs.

100.16.3 External Suppliers/Vendors Contracts

All LSUHNO suppliers/vendors who handle protected or restricted information shall acknowledge compliance with the LSUHNO information security procedures prior to accessing IT resources.

100.16.4 Non-Disclosure Agreements

LSUHNO IT shall confirm the existence of a Business Associate Agreement (BAA) with external contractors/suppliers before granting access to information classified as protected or restricted whenever applicable.

100.17 Separation From the University

100.17.1 User Separation

EIS shall be responsible for revoking access to information systems when user affiliation with the University has ended. Affiliation is determined by information in the HR system and other authoritative systems that manager user affiliations with the University. When it is determined that an employee represents a risk to the security of LSUHNO IT resources, all access shall be terminated immediately.

100.17.2 Procedures for Users Separating From the University Staff leaving employment shall return all LSUHNO property previously assigned including, but not limited to, all keys, access cards and all forms of employee identification.

100.18 IT Resource Security

100.18.1 Defending Against Unauthorized or Criminal Activity

All LSUHNO departments shall follow the LSUHNO Information Security Incident Response Procedure (Appendix C) by promptly reporting incidents.

100.18.2 Security Incident Procedures

All LSUHNO departments shall promptly report to EIS all suspected or actual information security incidents as defined by the LSUHNO Information Security Incident Procedure.

100.18.3 Investigating, Responding, and Reporting Information Security Incidents

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 incidents. Results of Information Security Incident investigations shall be thoroughly documented in security incident reports to be kept on file for at least six years. Incident reports shall include any and all recommendations to prevent recurrence of similar incidents.

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 New Orleans (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 been 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 break-

ins. 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.

B.1 External Affiliates

External Affiliates are users who are neither LSUHNO employees nor students, but require access to LSUHNO IT resources. Access to LSUHNO IT resources for external affiliates must be authorized by, and coordinated through, an affiliate sponsor.

B.1.1 External Affiliate Computer Accounts

Access to LSUHNO IT resources for external affiliates is provided so long as the access is a benefit to LSUHNO. Once an affiliate separates from LSUHNO, access to IT resources shall be revoked immediately.

B.1.2 New External Affiliations

Computer Accounts for external affiliates shall be granted once an affiliation is established. To establish an affiliation, the following must be provided:

a) A brief description of the relationship of the affiliation to LSUHNO and how access shall be of benefit to the University.
b) A description of the type of access required, e.g. e-mail, CLIQ, PeopleSoft, card access, etc.
c) An approximation of the number of individuals for whom access shall be required.
d) The name of the individuals who shall be the affiliation sponsors. The sponsors are responsible for coordinating with LSUHNO EIS on all matters relating to the affiliation. A minimum of two sponsors must be identified to establish an affiliation.
e) Acknowledgement that external user access to LSUHNO IT resources is provided so long as the access is a benefit to LSUHNO.
f) Acknowledgment that the sponsors assume responsibility to maintain affiliate status with LSUHNO through the Manage External Users web application.
g) Acknowledgment that the sponsors assume responsibility to terminate an affiliate's access whenever an affiliate's relationship with LSUHNO ends. The sponsors assume responsibility for all activity associated with the accounts of terminated affiliates until the user's access has been removed through the Manage External Users web application.
h) Acknowledgement that the sponsors are required to verify the status of each individual affiliate every three months in the Manage External Users web application.

B.1.3 Deactivating Access for External Affiliates

Accounts for external affiliates shall be deactivated at the end of the day on the termination date set on the External User record.

B.1.4 External Affiliate Records Maintenance

External Affiliate Sponsors are responsible for maintaining accurate demographics of the affiliates in the Manage External Users web application.

B.2 Vendor Accounts

Vendor accounts are used to provide short-term access to LSUHNO IT resources for third-party supporters or contractors.

B.2.1 Acquiring a Vendor Account

The owner of the resource (the LSUHNO contact) shall notify EIS that a vendor or contractor requires remote access to LSUHNO IT resources. Before creating the account, LSUHNO EIS shall determine the method to allow access to the resource. If it is decided that a vendor account is required, the account shall be set up according to EIS procedures. The LSUHNO contact shall designate at least two liaisons with the authority to request activation of the vendor account.

B.2.2 Vendor Account Requirements

Vendors and contractors must submit a signed copy of the LSUHNO vendor account agreement on company letterhead. The signed agreement shall be kept on file by EIS. When a vendor account is no longer needed, the resource owner shall notify EIS so the account can be deprovisioned.

B.2.3 Enabling a Vendor Account

Vendor account activation is processed through the LSUHNO Help Desk. The vendor shall notify a liaison of the need to activate the account. The liaison shall contact the LSUHNO Help Desk to open a ticket requesting activation. The ticket shall be processed by an EIS analyst. If the request is made outside regular working hours, the liaison shall instruct the Help Desk to call the EIS analyst on call. Vendor accounts shall be activated for up to 7 days. Activations for more than 7 days shall require business justification. The activation may be extended for up to 7 days at any time by the liaison opening a new Help Desk ticket.

B.3 Service, Lab, and Workstation Accounts

Service accounts are used to run applications or processes on LSUHNO IT resources. Lab and Workstation accounts are used to provide logons to lab computers and smart terminals.

B.3.1 Acquiring a Service, Lab, or Workstation Account

The resource owner shall notify EIS via email of the need for a service account. Service, Lab, and Workstation accounts are unique to specific business processes and shall not be reused or repurposed for any other application or process. The LSUHNO contact shall provide a list of IT

resources where the account shall be used so account restrictions can be enforced.

B.3.2 Service, Lab, and Workstation Account Restrictions

EIS shall create the service, Lab, or Workstation account with account restrictions and shall securely provide the resource owner with the account password. Service, Lab, and Workstation accounts neither expire nor follow all parts of the LSUHNO password policy. Service accounts shall not be used to obtain remote access to the LSUHNO network. When a service account is no longer needed the resource owner shall contact EIS so that the account can be deprovisioned.

B.4 Visitor Accounts

Visitor accounts are used to provide temporary wireless Internet access through the LSUHNO network infrastructure.

B.4.1 Visitor Account Requirements

At least two visitor accounts are provided to every LSUHNO computer support group. Visitor accounts are standard user accounts assigned to the lead supporter of the respective computer support groups. Supporters are responsible for setting the password on the account, setting appropriate expiration dates when the accounts are in use, and updating the description when the account is activated.

B.4.2 Enabling a Visitor Account

Requests to activate a visitor account shall be made to the local IT support group. EIS shall monitor the use of visitor accounts to ensure an appropriate expiration date is set on the visitor accounts and to limit the use of a visitor account to its intended purpose. Visitor accounts shall not be used to obtain remote access to the LSUHNO network.

B.5 Password Policy

LSUHNO Password Policy requires that:

B.5.1 Minimum password length and format shall be no less than ten (10) characters.

B.5.2 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 special characters (#, @, $ and _).

B.5.3 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.

C.1 Security Incidents

An information security incident is any use or attempted use of LSUHNO I.T. resources in violation of Federal or State laws or regulations or University policies. 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.

C.2 Incident Response Procedure

Information Security incidents are responded to as follows:

C.2.1 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.

C.2.2 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.

C.2.3 Post Incident Review for Major Incidents

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

Purpose

The purpose of this policy is to provide guidelines for the appropriate use and configuration of mobile devices and mobile storage devices as necessary to protect the network and\or information from unauthorized access or disclosure.

Scope

This policy covers all mobile devices used to access the LSU Health New Orleans (LSUHNO) network or mobile storage devices used to store LSUHNO information.

This policy covers all faculty, staff, students, vendors, contractors, guests and others who utilize a mobile device to access the LSUHNO network or store LSUHNO information.

Definitions

Mobile device: includes any device that is both portable and capable of collecting, storing, transmitting or processing electronic data or images.

Mobile storage device: includes storage media or any peripherals connected to a mobile device capable of storing LSUHNO information.

Personal mobile device: includes any mobile device that is not owned or issued by LSUHNO.

D.1 Requirements for the Use of Mobile Devices

1. Acceptable Use Policy. The use of personal mobile devices on the LSUHNO network is governed by CM-42, the policy regarding appropriate use of the LSUHNO network infrastructure.

2. Use of encryption. Any mobile device used to access or store LSUHNO data shall be encrypted if supported by the device.

3. Physical protection. Mobile devices owned or issued by LSUHNO shall not be left unattended and, where possible, shall be physically locked away or secured.

4. Device Passwords. All mobile devices accessing LSUHNO data shall use a PIN or passcode. Where supported, devices shall be configured to wipe corporate data after 10 invalid logon attempts.

5. Inactivity Timeout. All mobile devices that access LSUHNO data shall be configured to automatically lock the screen after no more than 10 minutes of inactivity and require a passcode, PIN, or password to unlock.

6. Virus protection. Any mobile device accessing LSUHNO data that is capable of using antivirus software shall have the software installed and configured to regularly update virus signatures.

7. Security Updates. Any mobile device accessing LSUHNO data shall be configured to check for application and operating system updates on a regular basis.

8. Termination of University relationship. All LSUHNO owned mobile devices must be returned immediately upon termination of the assigned user's relationship with LSUHNO. The mobile device shall be wiped by LSUHNO IT staff upon the user's separation from LSUHNO. All applications purchased by LSUHNO and all LSUHNO data shall be removed from personal mobile devices upon termination of the user's relationship with LSUHNO.

9. Misuse or Theft Any suspected misuse or theft of an LSUHNO owned mobile device shall be reported immediately to Enterprise Information Security and LSUHNO campus police.

10. Secure connectivity. Any sensitive information transmitted to or from a mobile device shall be encrypted.

11. Backups. All backups of mobile devices with LSUHNO data shall be encrypted.

12. Protection of information. Reasonable care shall be taken to avoid the unauthorized access to, or disclosure of, the information stored on, or accessed by, the device.