

CM-42 - Information Technology (IT) Infrastructure Policy

Statement of Purpose

The LSU Health Sciences Center New Orleans (LSUHSC-NO) and Health Care Services Division (LSUHSC-HCSD) information technology (IT) infrastructure supports mission-critical and business-critical services for patient care, education, public service, research, and administration.

LSUHSC-NO and LSUHSC-HCSD shall hereinafter be referred to as LSUHSC.

Staff, researchers, clinicians, students, and faculty depend on the LSUHSC IT infrastructure for the electronic classroom, telemedicine, healthcare, clinical and administrative database applications, high-speed data and image exchange, and collaborative initiatives with both internal and external entities.

The purpose of this document is to institute an enforceable policy to protect the performance, integrity, security, reliability, and continuity of vital services that rely on the LSUHSC IT infrastructure through good citizenship and legal and ethical use.

Statement of Applicability

This policy applies to any person or any device that connects to the LSUHSC IT infrastructure and is meant to augment, but not replace, any existing policy, laws, or regulations that currently refer to computing and networking services.

Any policy at a division or department level of the organization should build upon the foundation of this policy, and may be more restrictive than this policy, but should not be less restrictive.

All IT infrastructure strategic decisions shall be in concert with the appropriate leadership in the affected areas.

LSUHSC Enterprise Computer Services (ECS) provides management and operation of the IT infrastructure in partnership and cooperation with the major divisions of LSUHSC. All IT infrastructure designs must be coordinated and approved by ECS. All new network cable plants must adhere to the ECS cabling and wiring standards, and must be approved by ECS.

The owner of an LSUHSC user ID shall be held accountable for any violations associated with that ID, regardless of the ownership or the location of the equipment where the violation may have occurred.

Definitions and Terms

Authorized Use – Use of the IT infrastructure must be consistent with the instructional, research, public service, patient care, and administrative goals of LSUHSC, and for the express purpose of conducting business related to one's job duties.

Authorized User – Staff, student, faculty, contractor, vendor, or entity that has an official affiliation with LSUHSC and has been assigned a network user ID and/or has been specifically authorized to use an infrastructure resource by the group responsible for operating the resource.

Business Use/Need – That which is consistent with one's role in the organization.

Enterprise Computer Services (ECS) – The LSUHSC, Administration and Finance New Orleans, central computer services group. This group provides IT services that are used by the entire LSUHSC organization such as the network infrastructure, administrative applications, web services, E-mail infrastructure, IT security, etc. Other distributed IT groups in coordination with ECS provide IT services at the hospital, division, or department level.

LSUHSC Information Technology Infrastructure – Information technology (IT) is a compilation of products and services that turn data into functional, meaningful, available information. The IT infrastructure is the network, the communication physical media, the protocols, the associated software/applications/firmware, the hardware devices that provide connectivity, and all equipment attached thereto regardless of ownership or location.

Network – A network is that system of products and services by which all computers and peripherals are connected. Due to the current need for high-speed networking, it is critical that cables and wiring adhere to industry wiring standards to provide a reliable service.

Network User ID – A network account assigned by ECS Security that provides authentication and access to the LSUHSC network and applications on the IT infrastructure. A user must fill out an account application through his/her local supporter and sign a statement attesting to having read and understood the proper use of his/her user ID and password.

Policy Statement

Use of the LSUHSC IT infrastructure is a revocable privilege granted to those with an official affiliation with LSUHSC. Access to specific services on the IT infrastructure is based on a business need. Access to the IT infrastructure, and any components on the infrastructure, requires authorization. The LSUHSC IT infrastructure must be used in a manner consistent with protecting patient care and the critical business functions of the organization. No one should perform any activity on the IT infrastructure that undermines the public's confidence in LSUHSC to fulfill its mission.

Online Privacy Statement

Authorized LSUHSC staff may, at any time, for any reason, or without reason, access any device connected to the LSUHSC network such as a computer, its hard drives and component parts, monitor all contents, copy (download) any and all contents and use any such contents, for any purpose it deems necessary.

All users are advised that they should have no expectation whatsoever of privacy as to any transmission/communication or image generated, received by, sent by, or stored in a computer.

All users are advised that by using a computer on the LSUHSC IT infrastructure, they acknowledge that they are subject to the terms of this policy and that they give their unrestricted consent to the monitoring, copying, and unrestricted distribution of any transmission/communication or image generated, received by, sent by, or stored in the computer.

Acceptable Use Statement

All users of the IT infrastructure are expected to exhibit responsible behavior and shall:

- Comply with all federal and state laws, LSUHSC rules and policies, terms of computing contracts, and software licensing rules.
- Obtain authorization to use LSUHSC computing resources.
- Be held responsible for the use of their assigned user ID. Sharing of user IDs and passwords is prohibited.
- Obtain the proper authorization prior to accessing or sharing LSUHSC data.
- Actively participate and cooperate with ECS in the protection of the IT infrastructure against threats. For example, not opening E-mail from an unknown source, safeguarding passwords, reporting any violations of the acceptable use statement to the local support staff, and cooperating with the local support staff to keep security patches up to date on applications and computers.
- Take reasonable precaution to avoid introducing computer viruses into the LSUHSC network. For example, files downloaded from the Internet, received from E-mail, or brought in from outside LSUHSC must be scanned with ECS approved virus-scanning software. Anyone suspecting they may have a computer virus should contact their local support staff immediately.

All users of the IT infrastructure shall NOT:

- Engage in any activity that jeopardizes the availability, performance, integrity, or security of the IT infrastructure. Examples would be not installing FTP servers or web servers without consultation with ECS; not using peer-to-peer (P2P) applications that take up bandwidth for the downloading of music, games, and video; not releasing computer viruses or worms; and not deliberately or recklessly overloading access links or switching equipment through the use of streaming media such as web radio and other mechanisms.
- Use computing resources in a wasteful manner that creates a direct cost to LSUHSC. Some examples of waste are unnecessary backgrounds on E-mail taking up valuable storage space, spending time on the Internet for personal use, playing computer games, engaging in non-business related online chat groups, or printing multiple copies of documents.

- Use LSUHSC IT resources for personal monetary gain or commercial purposes not directly related to LSUHSC business or for functions that are not related to one's job.
- Install, copy, or use any software in violation of licensing agreements, copyrights, or contracts.
- Send copies of documents or include the work of others that are in violation of copyright law in electronic communications.
- Obtain or attempt to access the files or electronic mail of others unless authorized by the owner or as required for legitimate business need, security issues, or investigative purposes. Disclosure of any information obtained must abide by existing policy, laws, and regulations.
- Harass, intimidate, or threaten others through electronic messages.
- Construct a false communication that appears to be from someone else.
- Send or forward unsolicited E-mail to lists of people you do not know. It places considerable strain on the E-mail system. Bulk mailing of information can be selectively used for business-related communication but must be approved at a level appropriate to the scope and content of the information. Contact ECS for help with bulk mailings.
- Send, forward, or reply to E-mail chain letters.
- "Reply to all" to mass E-mail mailings.
- Retransmit virus hoaxes.
- Create or transmit (other than for properly supervised and lawful research purposes) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images.

Amendments and Revisions

This policy shall be amended or revised as the need arises.

Enforcement of Policy

Noncompliance with this policy could result in disciplinary action up to and including termination of employment, dismissal from an academic program, and civil or criminal liability.