LSU Health NEW ORLEANS
Office of the Chancellor

Chancellor's Memorandum
CM-42 – Information Technology (IT) Infrastructure

To: Vice Chancellors, Deans, Department Heads, Faculty, Staff, and Students

From: LSU Health Sciences Center New Orleans Chancellor

January 1, 2019. This memorandum supersedes CM-42 dated January 16, 2016.

Statement of Purpose

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

LSUHSC-NO and LSU-HCSD shall hereinafter be referred to as LSUHSC and HCSD, respectively, and collectively, as SYSTEM.

Staff, researchers, clinicians, students, and faculty depend on the SYSTEM 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.

Mobile devices such as smartphones (e.g. iPhone®, Android™ …) and tablets (e.g. iPad®, Samsung Galaxy Tab, or Google Nexus …) use the SYSTEM IT Infrastructure to improve the delivery of information for the purposes outlined above by combining significant computing and communication capabilities with portability and ease of use. At the same time, these devices introduce new risks to the integrity, availability and confidentiality of Data.

The purpose of this document is to institute an enforceable policy to protect the performance, integrity, security, reliability, and availability of vital services that rely on the SYSTEM IT Infrastructure through good citizenship and legal and ethical use and to provide guidelines for the appropriate use and configuration of personal computers, laptops, and mobile devices as necessary to protect the SYSTEM IT Infrastructure from unauthorized access or disclosure.

Statement of Applicability

This policy applies to any person using, or any device that connects to the SYSTEM IT Infrastructure and is meant to augment, but not replace, any existing laws, regulations, or policies 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 shall not be less restrictive.

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

LSUHSC Department of Information Technology (IT Department) provides management and operation of the SYSTEM IT Infrastructure in partnership and cooperation with the major schools and divisions of SYSTEM. All SYSTEM IT Infrastructure designs must be coordinated and approved by LSUHSC IT. All new network cable plants must adhere to the IT cabling and wiring standards, and must be approved by IT.

Prior to purchase, all proposed acquisitions (including but not limited to those made with donations, grants, and foundation funds) of IT software and hardware, including mobile devices and laptops, must be coordinated with the school- or division-designated IT representative for review, adherence to LSUHSC IT security standards, and approval.

The owner of any Network User ID issued by LSUHSC is accountable for any actions or usage that is associated with that ID, regardless of the ownership or the location of the equipment where the usage occurred.

Definitions and Terms

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

Authorized User (User) – Staff, student, faculty, contractor, vendor, or other that has an official affiliation with LSUHSC and/or HCSD and has been issued an LSUHSC Network User ID and/or has been specifically authorized to use an infrastructure resource by the group responsible for operating the resource. Network User IDs are authorized for activation by a major division's IT support staff. The Network User ID must be activated by the end User. All Network User IDs and Data, with the exception of Student Network User IDs and Data, are deleted upon voluntary or involuntary separation from SYSTEM). Student Network User IDs and Data are deleted 60 days after date of separation from LSUHSC. Student Network User IDs, with access to PeopleSoft Self Service, may continue to access PeopleSoft Self Service until 5 years after date of separation.

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

Connected – A device is considered Connected to the SYSTEM IT Infrastructure if it is plugged into a wired network jack on campus, connects to the LSUHSC wireless network on campus, remotely connects to the LSUHSC network via the Internet, telephone connection, or other remote mechanism.

- Examples of remotely connecting include but are not limited to using the remote.lsuhsc.edu VPN "Network Connect" option, logging on to Citrix (Desktop or PSDesktop) on campus, or using a mobile device that is on a cellular network and is enrolled in the LSUHSC MDM system.

- Methods of accessing the LSUHSC network that do not meet the definition of Connected include but are not limited to using the remote.lsuhsc.edu VPN with the "Web Connect" option, using Outlook Web Access (OWA) off campus, or logging on to Citrix (Desktop or PSDesktop) off campus. Any traffic generated from a non-Connected device to a Connected device can be monitored and captured but the device itself cannot be seen or accessed.

Data – Any information residing on the SYSTEM IT Infrastructure or held on any other IT Infrastructure on behalf of SYSTEM. This data includes files, documents, messages in any format, including e-mail messages and posts made on any Social Media site maintained by/for SYSTEM. All SYSTEM data created and/or maintained by a User is also subject to this Policy, even if the data is created and/or stored on the User's own personal computer, smartphone, or other personal device.

Department of Information Technology (IT Department) – The LSUHSC Administration central computer services group. This group provides IT services such as network infrastructure, administrative applications, web services, E-mail infrastructure, IT security, etc. that are used by the entire LSUHSC and HCSD organizations and other distributed IT groups in coordination with the IT Department to provide IT services at the hospital, school, division, or department level.

End-User Device – is any device that is capable of collection, non-volatile storage, transmission or processing of Data and employed by a User to access Data. Examples include but are not limited to desktop computers and Mobile Devices. This definition also includes storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to a mobile device or computer.

Information Technology (IT) Infrastructure – Information technology 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 (including but not limited to switches, access points, and routers), and all equipment (including, but not limited to, personal computers, laptops, PDAs, and smart phones) attached thereto regardless of ownership or location.

LSUHSC Information – Information received from LSUHSC that is not a public record as defined by LA R.S. 44.1 et seq., access to which is only required by one's employment by or enrollment at LSUHSC.

Mobile Device – includes any End-User Device that is portable. Examples include, but are not limited to laptops, smartphones (e.g. iPhone®, Android™ …) and tablets (e.g. iPad®, Samsung Galaxy Tab, or Google Nexus …). This definition also includes storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to a mobile device or computer.

Mobile Device Management Software (MDM) – A system intended to distribute applications, data, and configuration settings to mobile communications devices, such as tablets and smartphones. The intent of MDM is to optimize the security of a mobile communications network, while minimizing downtime. MDM addresses the concern of automatic caching or storing of Data and User credentials on a mobile device and allows administrators to manage the operation of smartphones and similar devices as effectively as is done with desktop computers. Visit https://www.lsuhsc.edu/admin/it/email/mobiledevices.aspx?submenuheader=2 or contact your school/division IT supporter for additional information.

Network – A network is that system of products and services by which all computers and peripherals are linked, whether wired or wireless.

Network User ID – Network accounts created by LSUHSC IT Information Security identify the User and provide authentication and access to the SYSTEM network and applications on the SYSTEM IT Infrastructure. Accounts are auto created following entry of personnel into any one of several authoritative sources (e.g. PeopleSoft, various external affiliations, etc.).

Personally-Owned Mobile Device or Computer – Includes any mobile device or computer that is not owned/purchased by LSUHSC or HCSD.

Protected Data – includes, but is not limited to,

- Personal identity information (PII): includes but is not limited to Social Security Numbers, credit card numbers, bank and credit union account numbers, health insurance plan identification numbers, driver's license numbers, dates of birth, and other similar information associated with an individual student or employee that, if misused, might enable assumption of that individual's identity ("identity theft") to compromise that person's personal or financial security.
- Protected health information (PHI): includes health information that is associated with at least one of eighteen identifiers that make the information "individually identifiable." The eighteen identifiers specified by HIPAA include name, address, SSN, date of birth, date of health care, and other elements. Health information about groups of people (population data, mean and median data, aggregate data, etc.) that cannot be related to individuals is not PHI.
- Student educational record information: includes records that are based on student status and maintained by LSUHSC or a party acting for LSUHSC. Access to student records is governed by the Family Educational Rights and Privacy Act (FERPA).

Public Wireless Network (Public WiFi) – The publicly accessible wireless network that is set up at the HCSD hospitals for access to the Internet by patients and patient families.

Restricted Data - Any information of such a sensitive nature, the access of which is limited to those individuals designated by management as having a need to know. It includes but is not limited to:

- Ongoing investigation files, pending litigation files, attorney-client privilege emails and files, files subject to litigation holds, psychotherapy notes, and files regarding disciplinary action.

SYSTEM IT Infrastructure – Any IT Infrastructure owned by or held on behalf of SYSTEM.

Policy Statement

Use of the SYSTEM IT Infrastructure is not a right but a privilege granted to those with an official affiliation with SYSTEM. Access to specific services on the SYSTEM IT Infrastructure is based on a business or educational need. Access to the SYSTEM IT Infrastructure, and any components on the SYSTEM IT Infrastructure, requires authorization by a User's supervisor or affiliation sponsor. Users of the SYSTEM IT Infrastructure shall have no expectation whatsoever of privacy.

The SYSTEM IT Infrastructure must be used in a manner consistent with providing patient care, educating healthcare professionals, conducting research and protecting the critical business functions of the organization that support these functions. No one should perform any activity on the SYSTEM IT Infrastructure that adversely affects these functions or undermines the public's confidence in LSUHSC or HCSD to fulfill their missions.

No Expectation of Privacy

Users shall have no expectation of privacy regarding any Data residing on the SYSTEM IT Infrastructure, even including Data on Personally-Owned Mobile Devices or Computers used by faculty, staff, students, or other Users in conducting business for or on behalf of SYSTEM, regardless of whether the Data was generated as the result of Authorized Use, incidental use, or if the use is not permitted by or described by this Policy.

Except in those circumstances in which access is appropriate to serve or protect operations within the

SYSTEM and to meet policy requirements, stored Data will not be accessed by anyone other than:

- The person to whom the account in which the Data has been stored is assigned; or
- The person to whom the device containing the stored Data has been assigned.

LSUHSC may access, monitor, or disclose as LSUHSC deems appropriate, any Data or transmission of Data, (including confidential or personal information), without notice to or consent from the User for any reason, including:

- Troubleshooting hardware and software problems, such as rerouting or disposing of undeliverable mail;
- Preventing or investigating unauthorized access and system misuse;
- Retrieving or reviewing for SYSTEM purposes SYSTEM-related information;
- Investigating reports of violation of SYSTEM policy or local, state, or federal law;
- Investigating reports of employee or student misconduct;
- Complying with legal requests for information (such as subpoenas and public records requests);
- Retrieving information in emergency circumstances where there is a threat to health, safety, or SYSTEM property involved.

LSUHSC, at its discretion, may disclose the results of any such monitoring to appropriate SYSTEM personnel, law enforcement, investigating agencies and may use those results in appropriate external and internal disciplinary actions and other proceedings.

By using a computer, mobile device, or application on the SYSTEM IT Infrastructure, all Users acknowledge that they are subject to the terms of this policy and give their unrestricted consent to the monitoring, copying, and unrestricted distribution of any transmission/communication or image generated, received by, or sent by a computer, mobile device, or application on the SYSTEM IT Infrastructure.

Data will be removed remotely from mobile devices enrolled with the mobile device management system (MDM) under the following circumstances:

- The mobile device is lost, stolen, or believed to be compromised.
- The mobile device belongs to a User that no longer has a working relationship with SYSTEM.
- The User decides to un-enroll from MDM.

Encryption Requirements

The IT Department shall develop and/or approve encryption standards and methods to be used to protect SYSTEM in accordance with NIST Special Publication SP 800-111 and other applicable and successor standards promulgated by appropriate authorities.

Only encryption standards and methods developed and/or approved by the IT Department shall be used to protect SYSTEM.

All Protected Data and Restricted Data shall be encrypted in accordance with standards and methods developed and/or approved by the IT Department regardless of where it is stored or transmitted unless documented alternative technical, administrative and/or physical controls that provide equivalent protection are in place.

All End-User Devices shall be encrypted in accordance with standards and methods developed and/or approved by the IT Department.

Acceptable Use Statement

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

- Comply with all federal and state laws, LSU System, LSUHSC and/or HCSD rules and policies, terms of computing contracts, and software licensing rules.
- Obtain authorization to use LSUHSC and/or HCSD computing resources from the owner of the resource.
- Refer to the Compliance Officer or his designee, anyone seeking access to sensitive areas or access to System IT infrastructure for the purposes of conducting an audit, inspection, examination, appraisal or any other type of review. Such access shall not be granted until approved by the Compliance Officer or his designee.
- Be held responsible for the use of their assigned Network User ID and any and all actions that are performed with that ID. Sharing of User IDs and passwords is prohibited.
- Register security questions and agree to the SYSTEM's acceptable use policy.
- Obtain authorization from the owner of Data prior to accessing or sharing LSUHSC and/or HCSD Data.
- Actively participate and cooperate with the IT Department in the protection of the SYSTEM IT Infrastructure against threats by using virus-scanning software, not opening E-mail from an unknown source, safeguarding passwords, reporting any violations of the acceptable use statement to the local IT support staff, and cooperating with the local IT support staff to keep security patches up to date on applications, mobile devices, and computers, and staying abreast of new security issues by completing information security training. Anyone suspecting they may have a computer virus should contact their local IT support staff immediately.
- SYSTEM-owned devices must be scanned with THE IT DEPARTMENT approved virus-scanning software.
- Use encryption on any mobile device (including storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to a mobile device) that stores protected or restricted data.
- All devices that access DATA must be able to be locked, such that unlocking requires the use of PIN, passcode, biometric, or password. Devices that support an automatic wipe should be set so that DATA is wiped after 10 invalid unlock attempts.
- Have all End User Devices that access DATA configured to automatically lock the screen after a period of inactivity that achieves the best balance between confidentiality and availability as determined by IT Department's risk assessment process.

- Immediately report any suspected loss, misuse or theft of a computer or mobile device to the LSUHSC Police, (504) 568-8999, and the LSUHSC Help Desk, (504) 568-HELP.
- Immediately report any suspected unauthorized access of SYSTEM IT Infrastructure or Data to the LSUHSC Help Desk, (504) 568-HELP.
- Register smartphones and tablets owned or issued by LSUHSC with the mobile device management system (MDM).
- Register Personally-Owned Mobile Devices that Connect with System IT Infrastructure with the LSUHSC mobile device management system (MDM).
- Take reasonable precautions to prevent unauthorized access to or disclosure of protected and restricted information stored on a mobile device.
- Encrypt any backups of mobile devices that contain protected or restricted information.
- Remove all LSUHSC Information from a personally owned computer or mobile device immediately upon termination of the assigned User's relationship with LSUHSC and/or HCSD.

<u>All users of the SYSTEM IT infrastructure shall NOT:</u>

- Reveal their Network User ID and password. LSUHSC and/or HCSD will never ask you to reveal your password
- Obtain or use another's Network User ID or password, or otherwise access DATA or SYSTEM IT Infrastructure to which authorization has not been expressly and validly given. Users shall not use another's User ID or password to hide their identity or attribute their use of Data or SYSTEM IT Infrastructure to another.
- Use non-LSUHSC E-mail to conduct official LSUHSC business unless authorized by the Chancellor.
- Engage in any activity that jeopardizes the availability, performance, integrity, or security of the SYSTEM IT Infrastructure. Examples include but are not limited to:
    - Adding, modifying, reconfiguring, or extending any component of the SYSTEM network such as hubs, routers, switches, wireless access points, firewalls, etc. or installing FTP, DHCP, or web servers without consultation with THE IT DEPARTMENT;
    - Intentionally or knowingly copying, downloading, installing, or distributing a computer virus, worm, "Trojan Horse" program, or other destructive programs, or otherwise harming systems or engaging in any activity that could reasonably and foreseeably disrupt services, damage files, cause loss of Data, or make unauthorized modifications.
    - Monopolizing or disproportionately using shared SYSTEM IT Infrastructure, overloading systems or networks with endless loops, interfering with others' Authorized Use, or degrading services by deliberately or recklessly overloading access links or switching equipment through downloading pictures or using streaming media such as web radio, games, videos, peer-to-peer (P2P) apps such as BitTorrent and Gnutella, and other mechanisms. These activities do not refer to legitimate business or school-related use of the SYSTEM IT Infrastructure.
    - Utilizing the SYSTEM IT Infrastructure to create, transmit, or otherwise participate in any pranks, chain letters, false or deceptive information, misguided warnings, pyramid schemes, or any fraudulent or unlawful purposes.
- Use computing resources in a wasteful manner that creates a direct cost to LSUHSC and/or HCSD. Examples include but are not limited to :
    - Unnecessary backgrounds on E-mail taking up valuable storage space,
    - Spending time on the Internet for personal use such as shopping, sports, entertainment, etc.,
    - Playing computer games,
    - Engaging in non-business related online chat groups,
    - Storing personal Data on LSUHSC and/or HCSD-owned systems,
    - Printing personal documents, or
    - Printing excessive copies of documents.
- Use SYSTEM IT resources for personal monetary gain or commercial purposes not directly related to LSUHSC and/or HCSD business or for functions that are not related to one's job.
- Use the Public Wireless Network for personal use during work hours. Examples include but are not limited to:
    - Accessing personal email
    - Accessing social media sites or chat groups

    - Online shopping and entertainment websites
    - Playing computer games
- 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 laws 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 any electronic means.
- 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. Bulk E-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 postmaster@lsuhsc.edu for help with bulk E-mailings.
- Send, forward, or reply to E-mail chain letters.
- Initiate or 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.
- Store unencrypted User IDs and passwords which allow access to the SYSTEM IT Infrastructure on mobile devices.
- Leave SYSTEM-owned mobile devices unattended.
- Circumvent or attempt to circumvent any administrative, physical or technical safeguard employed by SYSTEM to protect IT Infrastructure and Data.

Enforcement of Policy

The unauthorized or improper use of the SYSTEM IT infrastructure, including the failure to comply with this Policy will subject the violator to loss of privileges, disciplinary action, personal liability and/or criminal prosecution. In addition, LSUHSC may require restitution for any use of service, which is in violation of this Policy.