

**Medical School Information Technology (MSIT)
Security Policies and Procedure Acknowledgement Form**

The University of Texas Health Science Center at Houston's (UTHSC-H) information resources are owned by the university and are provided to accomplish the university's mission. Users must use university information resources appropriately to ensure availability and preserve information integrity and confidentiality. A user is anyone who is granted access to a university information resource, including, but not limited to faculty, students, residents, staff, alumni, retirees, continuing and distance education students, researchers, principal investigators, visiting faculty, business partners, contractors, vendors, consultants. Any electronic equipment, devices or media that a user connects to the university network or uses to process or store university information, including equipment, devices or media owned by the user or funded by another source, are considered university information resources for the purpose of compliance with laws, regulations and policies.

Use of university information resources is subject to UTHSC-H and University of Texas System (UT System) policies and state and federal laws, which include, but are not limited to:

- UTHSC-H Information Technology policies and procedures posted in the [IT Policy & Document Repository](http://it.uth.tmc.edu/cio/itpolicies.htm) (<http://it.uth.tmc.edu/cio/itpolicies.htm>);
- UTHSC-H Handbook of Operating Procedures (HOOP) [175](https://inside.uthouston.edu/hoop/policy.htm?id=1448198), Responsibility for the Use of Information Resources (<https://inside.uthouston.edu/hoop/policy.htm?id=1448198>);
- HOOP [180](https://inside.uthouston.edu/hoop/policy.htm?id=1448208), E-mail and Internet Usage (<https://inside.uthouston.edu/hoop/policy.htm?id=1448208>);
- UT System policy [165](http://www.utsystem.edu/policy/policies/uts165.html), UT System Information Resources Use and Security Policy (<http://www.utsystem.edu/policy/policies/uts165.html>).

Failure to comply may result in disciplinary action including termination of employment, professional/business relationship, or dismissal from school. Civil and/or criminal sanctions may apply.

I acknowledge I understand my role in protecting information resources. I will uphold/comply with applicable laws and the policies noted above, including the following:

1. University information resources must be secured from unauthorized, accidental or intentional access, modification or destruction.
2. University owned or managed information resources must be used only for university business. Personal data (examples include music, pictures, movies, etc.) is not to be stored locally or on any servers.
3. All assigned passwords to information resources including, but not limited to, network systems, computer accounts, encryption software, voice mail and long distance telephone codes must not be shared with anyone. Disclosing a password may result in immediate termination of employment, professional or business relationship, or dismissal from school.
4. Users should have no expectation of privacy regarding e-mail use, Internet use or other activities performed on, or information processed by or residing on, university information resources. All e-mail and Internet use can be monitored and stored along with the source and destination. Additionally, all incoming and outgoing email is being archived and is subject to the Texas Public Information Act.

5. Software, including electronic media or files, may not be downloaded, copied or otherwise used in violation of the licensing agreement and/or copyright.
6. All information resources and users are subject to random, unannounced inspection audits to ensure compliance with all university and UT System policies and state and federal laws.
7. It is the responsibility of all users to report any suspected or confirmed violations to appropriate management, to MSIT management, to the Chief Information Security Officer (ciso@uth.tmc.edu), or via the confidential compliance hotline (888-472-9868).
8. Users must complete all required initial and recurring information resource training.
9. For information resource support, please fill out the online form at the address below: <http://med.uth.tmc.edu/msit/mshelp.htm>
10. Unless an individual has been granted administrative or “power user” privileges by MSIT, only MSIT personnel can install, reconfigure or otherwise adjust any computer system hardware or software. These individuals include contractors, consultants and other UTHSC-H employees.
11. All users dealing with confidential or sensitive information, including but not limited to information covered by FERPA and HIPAA (such as PHI), must have a digital certificate. Digital certificates can be applied for at: <http://www.uth.tmc.edu/netcenter/middleware/digital-id/id-get.html>
12. All outgoing e-mail should be digitally signed if at all possible.
13. Identified patient care information in any form may be accessed only by authorized personnel. Using another person’s password to access or enter information into a patient’s clinical record is illegal. All e-mails containing identified patient data must be encrypted using a digital ID.
14. Confidential and sensitive information must be stored on appropriate network drives; do not save it on your local PC. If university business requires that it be saved on a portable device (e.g. external hard drive, USB device, DVD, CD, etc.), it must be encrypted, the device must be password protected, and it may only be saved temporarily.
15. All laptops must have full disk encryption as specified in the Laptop Security Policy (https://xfiles.uth.tmc.edu/Common/IT/Policies_and_Documents/Policies/LaptopSecurityPolicy.pdf), and all external hard drives and USB devices must have encryption capabilities as specified in the Portable Storage Device Policy (https://xfiles.uth.tmc.edu/Common/IT/Policies_and_Documents/Policies/PortableStorageDevicePolicy.pdf).
16. If you have been issued a university e-Token security key and you lose it, a \$36 replacement fee will be charged.
17. Do not disable your screen saver, or increase the 15 minute activation time. You may decrease the activation time.
18. Do not shut down your computers on Wednesday night so that Windows operating system and application updates are applied. Additionally, if you have a MAC, please do not shut your machine on the third Thursday of every month. During this maintenance window your computer may automatically reboot. Make sure you save all your working documents and log off your computer.
19. Leasing computers is a university standard. The computer leasing website is at: <http://med.uth.tmc.edu/msit/leasing/overview.htm>

- 20. All laptops, whether leased or purchased, need to be secured with a locking mechanism.
- 21. No computer or peripheral can be transferred from Surplus to the Department without explicit approval from MSIT.
- 22. No computer or peripheral should be moved without MSIT knowledge or approval.
- 23. When purchasing new computers, computer accessories, peripherals or software you will need to consult with MSIT in order to make sure that the item(s) are compatible with your computer and meet(s) the university security requirements.
- 24. Do not remove or tamper with anti-virus software or install any other anti-virus or firewall software without explicit approval from MSIT.
- 25. MSIT will provide support to university owned computers that are being used at home. University home computers will need to be brought in for MSIT to work on them. These computers will be given the lowest priority.
- 26. It is the user's responsibility to make sure that all data is backed up on the university home computers, and that the computer is up to date on anti-virus software and operating system security patches.
- 27. MSIT will help with minor printer problems, but a printer repair vendor must be contacted for warranty or any other repair work.
- 28. Specialized computers including those used in research can be exempt from 10, 16, 18, 22 and 24 above. Please contact MSIT in order to obtain the proper exemptions. Once exempted, the user must make sure that all data is backed up on the specialized computer, and that the computer is up to date on virus protection and security patches.

By signing this form, you acknowledge that you have read it completely and fully understand the policies described above.

Please print on the lines below:

LAST NAME: _____

FIRST NAME: _____

DEPARTMENT: _____

ROOM #: _____

SIGNATURE: _____ DATE: _____