

Information Resources User Acknowledgement Form

The University of Texas Health Science Center at Houston’s (UTHSC-H) information resources are owned by the university and belong to the people of the state of Texas. Use of information resources is granted to accomplish the university’s mission, and is subject to UTHSC-H and University of Texas System (UT System) policies and state and federal laws. These include, but are not limited to: UTHSC-H Information Technology policies and procedures posted in the [IT Policy & Document Repository](#); UTHSC-H Handbook of Operating Procedures (HOOP) [17.01](#), Responsibility for the Use of Information Resources; UT System policy [165](#), UT System Information Resources Use and Security Policy. Compliance with these measures is part of the university’s Information Security Program. The UTHSC-H president delegates oversight of the program to the Chief Information Officer (CIO). All UTHSC-H information resources and users of those resources are subject to the CIO’s authority and are required to comply with applicable polices and laws. A user is any UTHSC-H affiliate who requires access to a university information resource (examples of users include faculty, students, staff, alumni, retirees, residents, researchers, principal investigators, contractors, vendors, consultants). Failure to comply may result in disciplinary action including termination of employment, professional or business relationship, or dismissal from school. Civil and/or criminal sanctions may also apply.

I acknowledge I understand my role in protecting information resources and will uphold/comply with the following:

1. Access to university information resources must be secured from unauthorized intentional and/or accidental access. Unauthorized modification, disclosure and/or destruction of data are prohibited.
2. All passwords to information resources including, but not limited to, network accounts, computer accounts, encryption software, voice mail and long distance telephone codes are confidential and property of the state. Disclosing a password to anyone may result in immediate termination of employment, professional or business relationship, or dismissal from school.
3. University information resources are only to be used for official state purposes.
4. Users should have no expectation of privacy in e-mail or internet usage. All university e-mail and internet use can be monitored and both source and destination information can be captured.
5. Sensitive and confidential data must be stored on appropriate network drives. If it must be saved temporarily on a portable storage device (e.g. external hard drive, USB device, DVD, CD-ROM, etc.), it must be encrypted.
6. Software may not be copied or otherwise used in violation of licensing agreements and/or copyright.
7. Users are subject to random, unannounced inspection audits to ensure compliance with all university and UT System policies and state and federal laws.
8. It is the responsibility of all users to report any suspected or confirmed violations to appropriate management, to the Chief Information Security Officer (ciso@uth.tmc.edu), or via the confidential compliance hotline (888-472-9868).
9. All sensitive and confidential information, including research data, SSNs, and information protected by HIPAA and FERPA, must be protected in accordance with UTHSC-H policies, UTS 165 and state and federal laws.
10. Users must complete all required initial and recurring information resource training.

I agree to comply with all UTHSC-H security requirements and policies, UT System policies, and state and federal laws.

PRINT First Name _____ **Middle Initial:** _____

PRINT Last Name _____

SIGNATURE: _____

DATE: _____

INTERNAL USE ONLY

Employee ID: _____

Student A#: _____

House Staff ID: _____

Guest ID: _____

Guests who are contractors or consultants must also sign the [Contractor Confidentiality Acknowledgement](#) form.