UTHealth Houston

Information Resources User Acknowledgement Form

The University of Texas Health Science Center at Houston (UTHealth) information resources are owned by UTHealth and are provided to accomplish UTHealth's mission. Users must use UT Health information resources appropriately to ensure availability and preserve information integrity and confidentiality. A user is anyone who is granted access to a UTHealth 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.

Use of UTHealth information resources is subject to UTHealth and University of Texas System (U.T. System) policies and state and federal laws which include, but are not limited to: UTHealth Information Technology policies and procedures posted in the IT Policy & Document Repository; UTHealth Handbook of Operating Procedures (HOOP) – HOOP Policy 175 "Roles and Responsibilities for University Information Resources; HOOP Policy 180 Acceptable Use of University Information Resources; U.T. System (UTS) policy UTS165 "UT System Information Resources Use and Security Policy". Failure to comply with these policies may result in disciplinary action up to and including termination of employment, professional/business relationship, or dismissal from school. Civil and/or criminal sanctions may apply.

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

1. UTHealth 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, voicemail 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.***
3. UTHealth information resources are only to be used for UTHealth business, except as otherwise permitted by UTHealth or U.T. System policies or applicable state or federal laws.
4. Users should have no expectation of privacy regarding email use, internet use or other activities performed on, or information processed by or residing on, UTHealth information resources, except as otherwise provided by UTHealth or U.T. System policies or applicable state or federal laws.
5. Confidential data must be stored on appropriate network drives. If it must be saved on a portable device (e.g. external hard drive, USB device, DVD, CD, etc.), it must be encrypted and saved only temporarily.
6. Software or electronic media or files (e.g. music, videos, e-books) may not be downloaded, 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 UTHealth and U.T. System policies and state and federal laws, except as otherwise provided by UTHealth or U.T. System policies or applicable state or 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 (its@uth.tmc.edu), or via the confidential compliance hotline (888-472-9868).
9. All confidential information, including research data, SSNs, and information protected by HIPAA and FERPA, must be protected in accordance with UTHealth policies, U.T. System Policy 165 and state and federal laws.
10. Users must complete all required initial and recurring information resource training.
11. I attest that I will not store Protected Health Information (PHI) on non-UTHealth managed computers.

PRINT First Name ____

PRINT Middle Initial: _____

PRINT Last Name ____

SIGNATURE: ____

DATE: ____

Please provide government-issued photo ID number and internal ID If known:

☐ Employee ID: ______________________

☐ Student emplid: ____________________

☐ Resident/House Staff ID: _____________

The following information is needed for password management and Two-factor authentication:

Password recovery e-mail address: ____

Mobile phone number: (   ) ________________________________