UNIVERSITY of HOUSTON | GRADUATE SCHOOL

ApplyWeb Access Request

Use this form to request access to graduate applications. Requests should be made for all graduate admissions advisors, faculty evaluators, executives and their designees who oversee graduate admissions.

Personal Information: To be filled out by requestor

Last Name _____ First Name _____

PS ID _____ Job Title _____

UH Email _____ UH Phone _____

Admissions Role: Please choose the role that most closely describes your current involvement in graduate admission. Explanations of roles can be found on page 2.

Role

- ☐ Admissions Advisor
- ☐ Faculty
- ☐ Program Lead/Director
- ☐ Department Chair
- ☐ Graduate Dean
- ☐ Chair/Dean Designee _____

Areas of Access: Indicate what colleges and programs you will require access to. If you require access to multiple programs, please indicate below. If there is not enough space, please attach the full list. **Please only list the areas you currently review applications for. For example, if you are faculty in Mathematics, you will only need access to Mathematics, not all of NSM.**

Program _____

Program _____

Program _____

Department _____

Department _____

College _____

Confidentiality Form: In addition to this form, all first time access requests to ApplyWeb must be accompanied by a UH confidentiality form. Please certify that the form has been sent.

Please check : ◯ UH Confidentiality Form submitted to Graduate School on _____

◯ UH Confidentiality Form is included

Approvals: All signatures must be present for request to be processed.

Supervisor

Email Phone

Signature: _____ Date

Graduate Dean/ Designee

Signature: _____ Date

System Security Administrator
UHGS Use only

Date Received: _____ Access:_____ Area: _____

Signature: _____ Print Name: _____

Definitions: Please refer to the following definitions to ensure that you request the correct access.

Roles

Academic Advisor - Typically a staff member. Assembles applications for faculty review. Will need access to add/remove documents at applicant's request; edit applicant information.

Faculty - Evaluates applications either individually or as a part of a committee. Does not make changes to applications.

Program Lead/Director - Evaluates applications either individually or as a head of a committee. Makes the initial decision to admit/deny applicant.

Department Char - Reviews program's decisions, affirms and send to Dean or returns to program for re-evaluation.

Graduate Dean - Final decision-maker at the College level. Affirms decision or sends applicant back to department for re-revaluation.

Chair/Dean Designee - Completes data entry on the part of the department chair or graduate dean. Please include the name of the person you are a designee for.

After filling out this form, please can and e-mail it to gradschool@uh.edu

Please notify the Graduate School about any changes in the Staff's employment Record, including termination and change of department so that we can update ApplyWeb access accordingly.

Confidentiality Statement - Governing UH Policy

I understand that data obtained from any UHS system is to be considered confidential and is NOT to be shared with anyone not previously authorized to receive such data.

Manual of Administrative Policies and Procedures
see MAPP Policy 10.03.01
at http://www.uh.edu/mapp/10/100301.pdf

I. PURPOSE AND SCOPE - This document outlines the responsibilities of users of University of Houston computing equipment and its associated network environment. The purpose of this document is to comply with UH System Administration Memorandum 07.A.03, University of Houston Information Security Manual, Computing Facilities User Guidelines, and other applicable local, state and federal requirements. These directives apply to all users of University of Houston computing equipment and related computing networks.
II. POLICY STATEMENT - University of Houston computing, communication and classroom technology resources provide computing services for the university community in support of the institutional mission .The university is responsible for ensuring that all such systems and resources are secure; i.e. that hardware, software, data and services are protected against damage, theft or corruption by individuals or events, internal or external to the university. It is the responsibility of each University of Houston computer user to avoid the possibility of misuse, abuse, or security violations related to computer and network use. Each user is responsible for becoming familiar and complying with guidelines, policies and procedures relating to university computing equipment and systems. This familiarity must be refreshed at every opportunity; at a minimum familiarity with security policies and guidelines shall be reviewed no less often than annually.
III.DEFINITIONS - Definitions of terms used in this policy may be found in the Glossary of Information Technology Terms located in the Information Technology MAPP section at http://www.uh.edu/mapp/10/100000.htm.ormation Technology Terms located in th
IV. POLICY PROVISIONS -
A. All multi-user/centrally maintained computer systems (i.e. computer systems not assigned to individuals but available for multiple users) requiring log-on and password shall have an initial screen banner reinforcing security requirements and reminding users of their need to use computing resources responsibly. Under State of Texas Department of Information Resources guidelines, systems not requiring unique user identification are exempt from this requirement.
B. Users of computers and computing systems must respect the privacy of others. For example, users shall not seek or reveal information on, obtain copies of, or modify files, tapes, or password belonging to other users nor may users misrepresent others. Computer accounts are assigned to individuals who are accountable for the activity on that account. Account holders are encouraged to change their passwords frequently to ensure the security of their accounts.
C. Computer account holders will be provided with updated user requirements messages when it becomes necessary. All users of computer systems and computing resources are responsible for reading and understanding requirements and responsibilities. Most software is protected against duplication by copyright or license. Users must abide by the laws protecting copyright and licensing of programs and data. University users shall in no case make copies of a licensed computer program to avoid paying additional license fees or to share with other users. For information regarding the terms of licensing agreements held by the University of Houston, contact the IT Support Center.
D. Users must respect the intended university business or academic purpose for which access to computing resources is granted. Examples of inappropriate use of university computing resources include, but are not limited to, use for personal or corporate profit, or for the production of any output that is unrelated to the objectives for which the account was issued.
E. Users must respect the integrity of computing systems. For example, users shall not intentionally develop or use programs that harass other users, infiltrate a computer or computing system, or damage or alter the software components of a computer or computer system. Any suspected irregularities discovered in system accounting or system security should be reported to the appropriate system administrator and to the information security officer so that steps can be taken to investigate and solve the problem.
F. Users must respect the shared nature of computing resources. For example, users shall not engage in inefficient and/or wasteful computing practices such as unnecessary printing, performing unnecessary computations, or unnecessarily using public workstations or network connections.
G. Users must respect the rights of other users. For example, users shall not engage in any behavior that creates an intimidating, hostile or offensive environment for other individuals.
H. Facility Supervisors and other custodians of computers are responsible for taking steps to reasonably ensure the physical security of university hardware, software and data entrusted to their use.
I. Each computing facility may have additional guidelines for the use of particular types of computer accounts, or for use of that facility Some facilities are restricted in use to student, faculty, staff members, and guests of a particular department. It is the user's responsibility to read and adhere to these guidelines.
V. NOTIFICATION OF USER RESPONSIBILITES
A. University policies and protocol covering responsibilities of users of computing resources shall be distributed by the Department of Information Technology to users when they are issued a computer account. Computer account holders will also be provided with updated user requirement messages when it may become necessary.
B. Such policies shall also be published in faculty staff, and student handbooks.
C. A banner summarizing user responsibilities and security guidelines will precede logging onto computer systems.
D. The comprehensive University of Houston Information Security Manual is located in key Information Technology offices and through the University of Houston Home Page.
E. All users of computer systems and computing resources are responsible for reading and understanding these requirements and their responsibilities. Any questions regarding requirements and responsibilities should be referred to the information security officer in Information Technology.
VI. VIOLATIONS - Threats to computing, network, or telecommunications security, whether actual or potential or illegal activities involving the use of university computer, network, or telecommunications systems, shall be reported tot he Information Technology Security Officer (or designee) or, in his absence, to the Chief Information Officer. Illegal activities may also be reported directly to a law enforcement agency.
For more information, please see MAPP 10.05.02 Security Violations Reporting.

I have read and understood the information on this form, and I agree to comply with the rules as stated therein:

Signature _____ Date _____