

## Security eForm. How to start a request?

1. Start by logging in to Campus Solutions.



2. Ensure you can see the CS security form icon. If you don't see the icon, please email [sa-security@uh.edu](mailto:sa-security@uh.edu) with your emplid.

CS Security eForm



Pending Approvals

3. 'Start Security Access Request' from the left-hand menu.

A screenshot of the 'UH CS Security Access Request' menu. The menu has a title bar and several options: 'Instructions', 'Start Security Access Request' (highlighted with a red box), 'Update a Request', 'View a Request', and 'Evaluate a Request'. Each option has a small icon to its left.

4. The following screen comes up. Validate items 1 through 6.

A screenshot of the 'UNIVERSITY of HOUSTON' Security Access Request form. The form is titled 'Access Request : Page 1 of 3'. It contains several sections: 'Requester' (with fields for User ID, Name, College/Department, Email Address, Basic Access Existing User, Job Title, and Phone), 'Request Access For' (with fields for Self, Manager Name, Manager Email, Manager PeopleSoft ID, and Manager Phone), and 'General Request Information' (with fields for Short Term Access Request and Student Worker). Red circles with numbers 1 through 6 are overlaid on the form to indicate specific validation points: 1. User ID field, 2. Self checkbox, 3. Manager Name field, 4. Manager PeopleSoft ID field, 5. Short Term Access Request checkbox, and 6. Student Worker checkbox.

5. Click 'Next'

6. Following screen comes up. For items 1 and 2, if you need full access to either DOB or SSN, please complete the justification box, which will pop up. Toggle buttons 3 to 11 to request access for the respective modules.

Request Access For

PeopleSoft ID  Name

Display of Social Security Number (SSN) & Date of Birth (DOB)

Set search screens to display ONE of the following for SSN and DOB. Default setting is Partial display for both SSN (last 4 digits) and DOB (Month/day)

1 Social Security Number  2 Date of Birth

Modules

All approve access requests will grant view only access to the Student Services Center, Student Biographical data, UHS Account Summary and Customer Accounts via the UHCSM\_CC\_GENERAL and UHCSM\_SF\_GENERAL roles.  
For users needing additional access to a specific module, please switch the toggle to "Yes" to select available options.

3 Academic Advising <input type="checkbox"/> No	7 Student Business Services <input type="checkbox"/> No
4 Admissions <input type="checkbox"/> No	8 Student Records <input type="checkbox"/> No
5 Campus Community <input type="checkbox"/> No	9 Institutional Research <input type="checkbox"/> No
6 Financial Aid <input type="checkbox"/> No	10 PeopleTools <input type="checkbox"/> No
11 Are you requesting Slate Roles? <input type="checkbox"/> No	

7. If you toggled yes for a module, the page would expand to show access options for the selected module/s. For each of the access toggled in area marked 1, you can find its required training in area 2. If the access you are looking for is not on a toggle, you can use the 'other' (marked as 3) box to write in the access needed. Click Next.

Modules

All approve access requests will grant view only access to the Student Services Center, Student Biographical data, UHS Account Summary and Customer Accounts via the UHCSM\_CC\_GENERAL and UHCSM\_SF\_GENERAL roles.  
For users needing additional access to a specific module, please switch the toggle to "Yes" to select available options.

Academic Advising <input type="checkbox"/> No	Student Business Services <input type="checkbox"/> No
Admissions <input type="checkbox"/> No	Student Records <input checked="" type="checkbox"/> Yes
Campus Community <input type="checkbox"/> No	Institutional Research <input type="checkbox"/> No
Financial Aid <input type="checkbox"/> No	PeopleTools <input type="checkbox"/> No
Are you requesting Slate Roles? <input type="checkbox"/> No	

Student Records

Required training BEFORE access is granted 2

Basic Access: SAXVM  
Enrollment Access: SAREMB  
Program/Plan Update: SARSRW  
Class Scheduler: SARCMU  
Graduation Processing: SAXGRT  
Service Indicators: SAXSIB

[UH Campus Solutions Training Site](#)

For Student Records access assistance contact: [UHSRSEC@UH.EDU](mailto:UHSRSEC@UH.EDU)

Basic SR Access Yes

Enrollment Access ☐ No 1

Program/Plan Update ☐ No

EAB Navigate

UHS Document Attachment (specify below) ☐ No

Class Scheduler ☐ No

Graduation Processing ☐ No

Other 3

8. If you toggled yes for module 11 ('Are you requesting Slate Roles?'), the next page shows the Slate Roles and Permissions that can be requested. Click Next.

Slate Roles

Are you requesting Slate Roles? ☒ Yes ☐ No

Admissions Admin Staff ☐ No

Admissions IT ☐ No

Admissions IT Grad Assistant Student Worker ☐ No

Bauer COB ☐ No

Campus Administrator ☐ No

Communication Specialist ☐ No

Counselor Recruiter ☐ No

Research Reporting ☐ No

(+) Inbox - Email ☐ No

(+) Inbox SMS Roles ☐ No

Other

Department Manager ☐ No

Department Manger 2 ☐ No

Event Coordinator ☐ No

General View ☐ No

Grad Assistant Student Worker ☐ No

Optometry Campus Administrator ☐ No

Research Analyst ☐ No

Student Ambassador ☐ No

Custom Slate Permissions

Admissions Read ☐ No

Admissions Write ☐ No

Integration Source Formats Read ☐ No

Integration Source Formats Write ☐ No

9. Complete the Acknowledgement section. Click Submit. Once the form is submitted, it is routed to your Manager for approval.

Confidentiality Statement

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 10.02.01 at <http://www.uh.edu/mapp/10.02001.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 07A.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 operations 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 in 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. It is not user's responsibility 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 [www.uh.edu/mapp/10.00000.pdf](http://www.uh.edu/mapp/10.00000.pdf)

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 sign-on and password shall have an inter-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 computer and computing systems must respect the privacy of others. For example, users shall not view or reveal information on, obtain copies of, or modify files, bases, or passwords 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 enhance 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. User 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 appropriate use of university computing resources include, but are not limited to, use for personal or corporate profit, or for the production of any school 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, interfere a computer or computing system, or damage or alter the software components of a computer or computer system. Any suspected malfeasance 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. Faculty, 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 RESPONSIBILITIES

A. University policies and procedures 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 download logging onto computer systems.

D. The comprehensive University of Houston Information Security Manual is located in the Information Technology Office 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 or 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 to the 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 10.02.02 Security Violations Reporting.

Action Items

Acknowledgement

☒ Yes ☐ No

By selecting the toggle to "Yes", I indicate that I have read and understood the information on this form, and I agree to comply with the rules as stated therein.

☒ Yes ☐ No

Check here to confirm employee needs access to education records in order to perform their official educationally-related duties.

7 Comments

FYI. Once your access has gone through all the approvals, and the Campus Security Administrator(s) (CSA) has processed your request, it is considered complete. You will receive an email like the following:

## Form Admin Tool

Form ID 240718      DateTime 10/28/2025 11:45:02.000000AM

To: [REDACTED]  
CC:  
BCC:

UNIVERSITYof HOUSTON

Your Form ID: 240718 - Campus Solutions Access Request and/or Slate Access Request has been completed.

To view the request, log into AccessUH, click on Campus Solutions, then the 'CS Security Form' tile. Then, select 'View a Request' from the left-hand menu. Enter the Form ID. Click search.

If you have any questions about this request, please contact the Campus Solutions Security Office at [sasecrt@central.uh.edu](mailto:sasecrt@central.uh.edu).

For inquiries about Slate Security, contact Gayle King.

**Comments:**

