

# 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.



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

Access Request: Page 1 of 3

UNIVERSITY of **HOUSTON**

Before PeopleSoft Campus Solutions access can be granted, the user must have the following information available for the form to be completed:

1. PeopleSoft ID number of the person you are requesting access for – This person should be an active employee or a Person of Interest (POI)
2. College Business Administrator (CSA) of the person you are requesting access for.
3. Have taken training session (if required)

**Assistance Information**

For assistance with the form or security access questions, please email [sa-security@uh.edu](mailto:sa-security@uh.edu).

For assistance with training, please contact Pamela Ogden, 832-842-9606, [progden@uh.edu](mailto:progden@uh.edu) OR navigate to HR's training information site.

**Please note:** An automated process removes Campus Solutions access when a user transfers or terminates from a position. Access to P.A.S.S. and Student Self-Service will remain active and available.

**Requester**

User ID  
Name:  3  
College/Department:  College of  
Email Address:  J  
Basic Access Existing User:  Y

Job Title:  Manager, Department  
Phone:  713-520-1022

**Request Access For**

2 Self  Yes   
3 Manager Name:   
Manager Email:

4 Manager PeopleSoft ID:   
Manager Phone:  713-520-1022

**General Request Information**

5 Short Term Access Request  Yes  No  
6 Student Worker  Yes  No

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 [REDACTED] Name [REDACTED]

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.

<b>3</b> Academic Advising <input type="checkbox"/> No	<b>7</b> Student Business Services <input type="checkbox"/> No
<b>4</b> Admissions <input type="checkbox"/> No	<b>8</b> Student Records <input checked="" type="checkbox"/> Yes
<b>5</b> Campus Community <input type="checkbox"/> No	<b>9</b> Institutional Research <input type="checkbox"/> No
<b>6</b> Financial Aid <input type="checkbox"/> No	<b>10</b> PeopleTools <input type="checkbox"/> No

**11** Are you requesting State Roles?  No

[Previous](#) [Next](#) [Save](#)

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 State Roles?  No

**Student Records**

**Required training BEFORE access is granted**

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

**2**

UH Campus Solutions Training Site

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

**1**

Basic SR Access <input checked="" type="checkbox"/> Yes	Class Scheduler <input type="checkbox"/> No
Enrollment Access <input type="checkbox"/> No	Graduation Processing <input type="checkbox"/> No
Program/Plan Update <input type="checkbox"/> No	
EAB Navigate <input type="text" value=""/>	
UHS Document Attachment (specify below) <input type="checkbox"/> No	

**3**

Other

[Previous](#) [Next](#) [Save](#)

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? <input checked="" type="checkbox"/> Yes <input type="checkbox"/>	Admissions Admin Staff <input type="checkbox"/> No	Department Manager <input type="checkbox"/> No
Admissions IT <input type="checkbox"/> No	Department Manager 2 <input type="checkbox"/> No	Event Coordinator <input type="checkbox"/> No
Admissions IT Grad Assistant Student Worker <input type="checkbox"/> No	General View <input type="checkbox"/> No	Grad Assistant Student Worker <input type="checkbox"/> No
Bauer COB <input type="checkbox"/> No	Optometry Campus Administrator <input type="checkbox"/> No	Research Analyst <input type="checkbox"/> No
Campus Administrator <input type="checkbox"/> No	Student Ambassador <input type="checkbox"/> No	
Communication Specialist <input type="checkbox"/> No		
Counselor Recruiter <input type="checkbox"/> No		
Research Reporting <input type="checkbox"/> No		
(+) Inbox - Email <input type="checkbox"/> No		
(+) Inbox SMS Roles <input type="checkbox"/> No		
Other <input type="text"/>		

#### Custom Slate Permissions

Admissions Read <input type="checkbox"/> No	Integration Source Formats Read <input type="checkbox"/> No
Admissions Write <input type="checkbox"/> No	Integration Source Formats Write <input type="checkbox"/> 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 UH 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 10.02.21 at <http://www.uh.edu/mapp/10.020001.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 STA-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 resources.

**II. POLICY STATEMENT** - University of Houston computing, communication and information 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, annually with security policies and guidelines that are revised or 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/10.020000.pdf](http://www.uh.edu/mapp/10.020000.pdf).

#### IV. POLICY PROVISIONS

- A. All university-maintained computer systems (i.e., computer systems not assigned to individuals but available for multiple users) requiring log-in and password shall have an initial screen banner reminding 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 see or reveal information on, obtain copies of, or modify files, tapes, or passwords belonging to other users, nor may users intercept messages of 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 protect 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. Heat software is protected against duplication by copyright or license. Users must abide by the laws protecting copyrights and licensing of programs and data. University users, 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 purposes 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 engage in inefficient and/or wasted computing practices such as unnecessary printing, performing unnecessary computations, or unnecessarily using public installations or network connections.
- F. Users must respect the shared nature of computing resources. For example, users shall not engage in any behavior that creates an intimidating, hostile or offensive environment for other individuals.
- 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 students, 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 practices 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 appear 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 to the Information Technology Security Officer (or designee) or, in his absence, to the Chief Information Officer. Legal activities may also be reported directly to a law enforcement agency.

For more information, please see MAPP 10.02.22 Security Violations Reporting.

#### Action Items

Acknowledgment	By checking 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
1 <input type="checkbox"/> No	
2 <input type="checkbox"/> No	Check here to confirm employee needs access to education records in order to perform their official educationally-related duties

#### F. Comments

Search  Previous  Next

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      Date Time 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 [sasecrty@central.uh.edu](mailto:sasecrty@central.uh.edu).

For inquiries about Slate Security, contact Gayle King.

### Comments:

