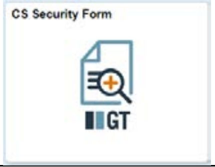
Security eForm. How to initiate a request for self?

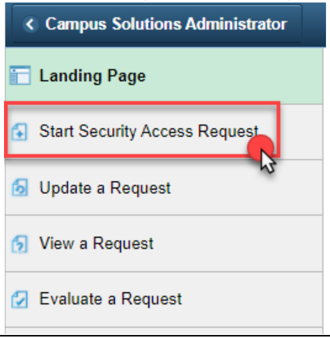
Note: At this time access can only be requested online for Student Records and Academic Advising. For other access requests, please complete the paper security form, **https://tinyurl.com/y449dr5z**.

1. Start by logging in to Campus Solutions.

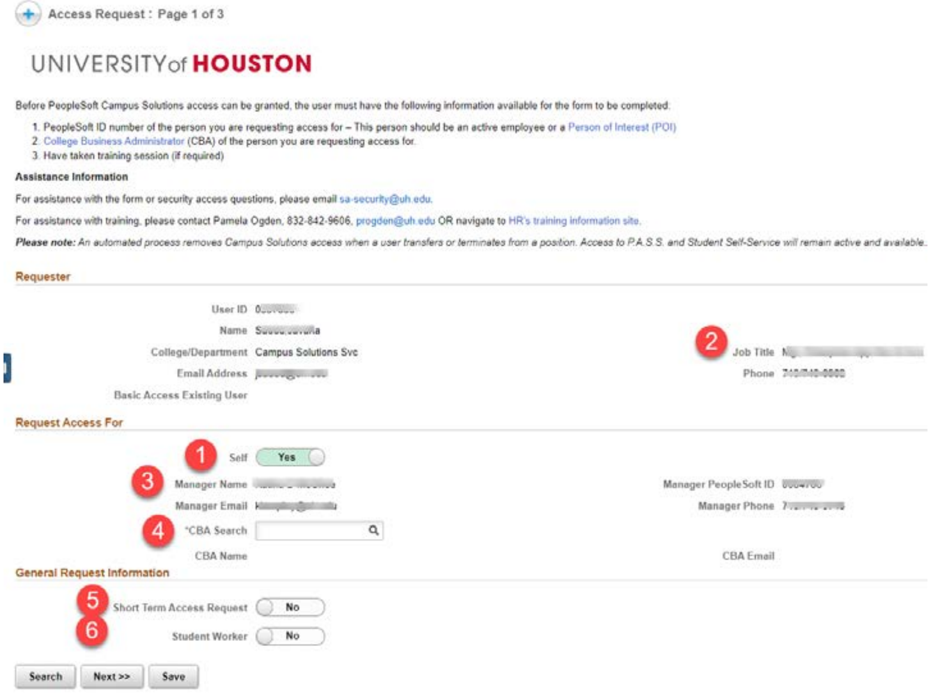
2. Ensure you can see the CS security form icon. If you don't see the icon, please email sa-security@uh.edu with your emplid.



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



4. Following screen comes up. Validate items 1 through 6. Please contact your Manager to find out who is the CBA for your department.



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 (CBA) 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.

For assistance with training, please contact Pamela Ogden, 832-842-9606, 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 [redacted]
Name [redacted]
College/Department Campus Solutions Svc
Email Address [redacted]
Basic Access Existing User

Job Title [redacted]
Phone [redacted]

Request Access For

Self Yes
Manager Name [redacted]
Manager Email [redacted]
*CBA Search
CBA Name

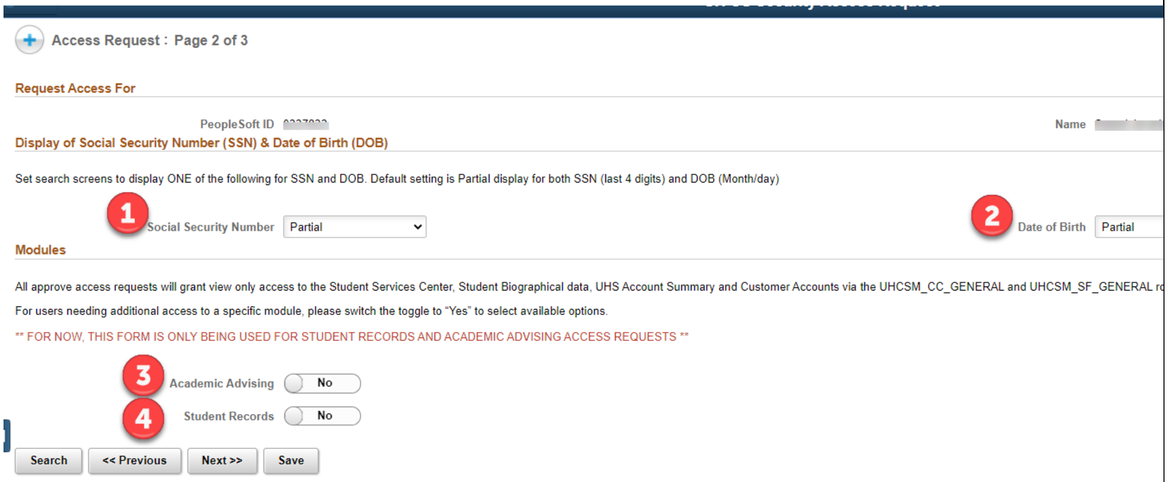
Manager PeopleSoft ID [redacted]
Manager Phone [redacted]
CBA Email

General Request Information

Short Term Access Request No
Student Worker 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 button 3 and/or 4 to request access for Academic Advising and/or Student Records.



Access Request : Page 2 of 3

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: Partial

2 Date of Birth: Partial

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 r

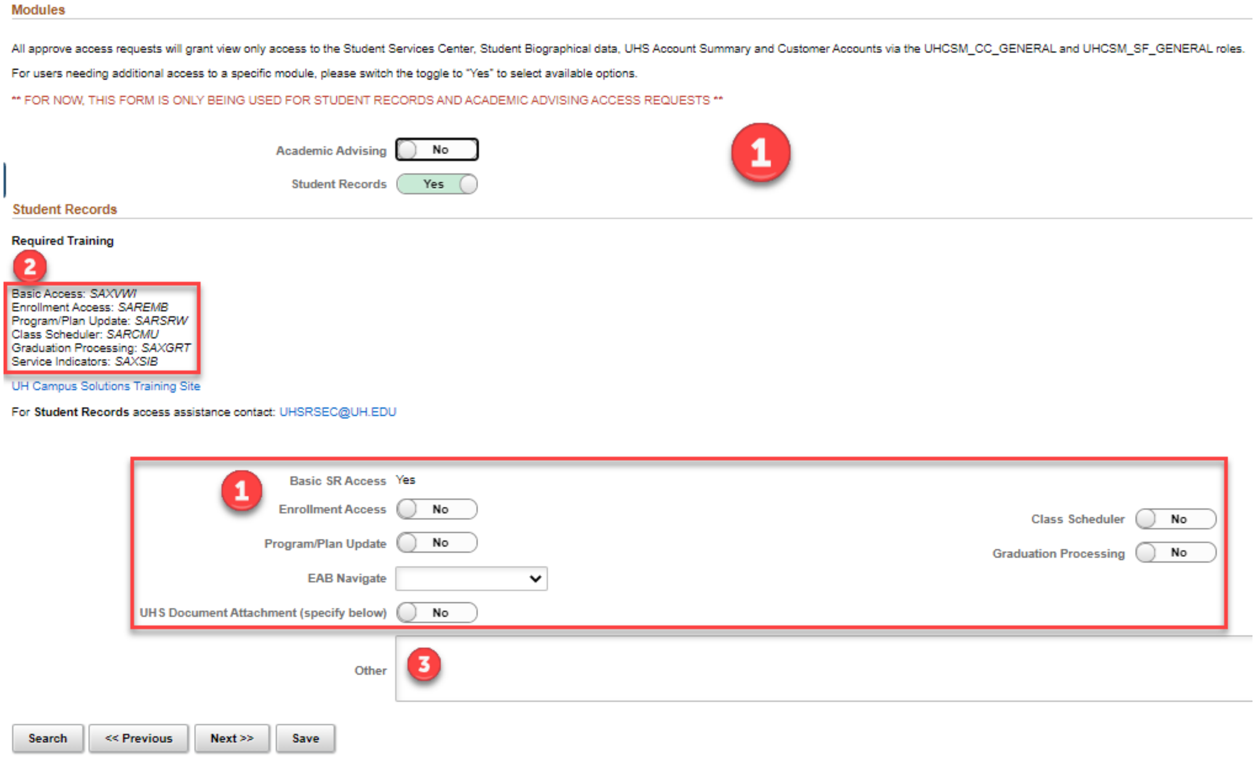
For users needing additional access to a specific module, please switch the toggle to "Yes" to select available options.

** FOR NOW, THIS FORM IS ONLY BEING USED FOR STUDENT RECORDS AND ACADEMIC ADVISING ACCESS REQUESTS **

3 Academic Advising: No

4 Student Records: No

7. If you toggled yes for either Student Records or Academic Advisement, the page will expand to show access options for the selected module/s. For each of the access toggle 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 needs. 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.

** FOR NOW, THIS FORM IS ONLY BEING USED FOR STUDENT RECORDS AND ACADEMIC ADVISING ACCESS REQUESTS **

Academic Advising: No

Student Records: Yes

1

Student Records

Required Training

2

Basic Access: *SAXVWI*
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

1

Basic SR Access: Yes

Enrollment Access: No

Program/Plan Update: No

EAB Navigate:

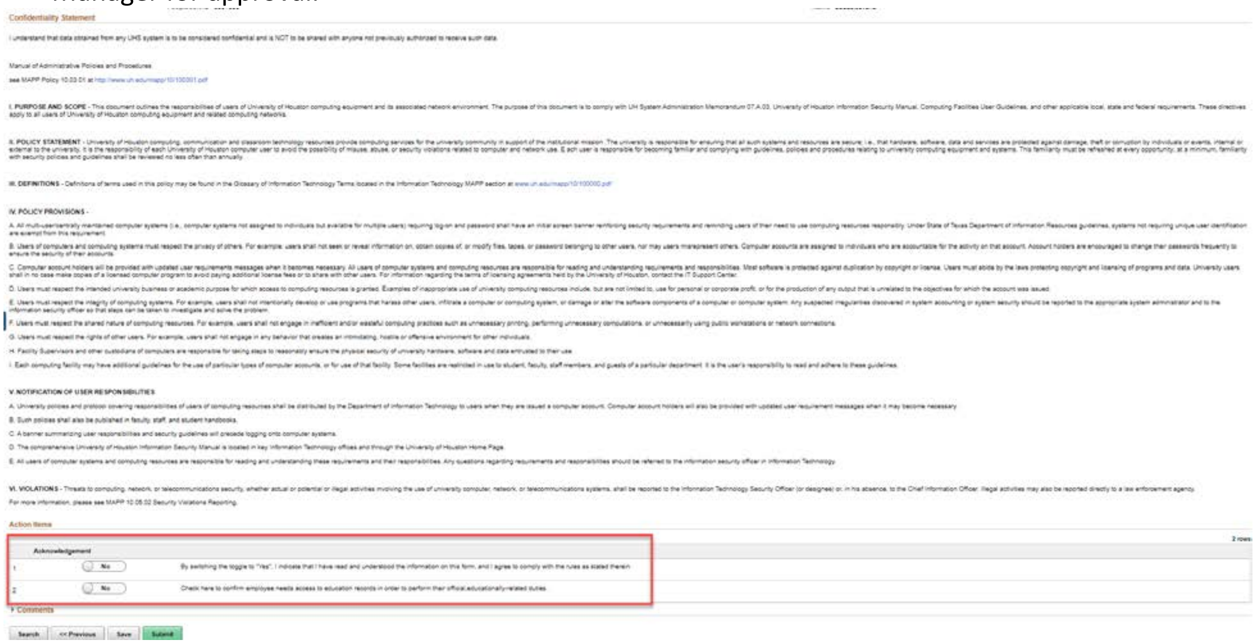
UHS Document Attachment (specify below): No

Class Scheduler: No

Graduation Processing: No

Other: 3

8. 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 10.03.01 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 www.uh.edu/mapp/10/100000.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 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 RESPONSIBILITIES

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 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.

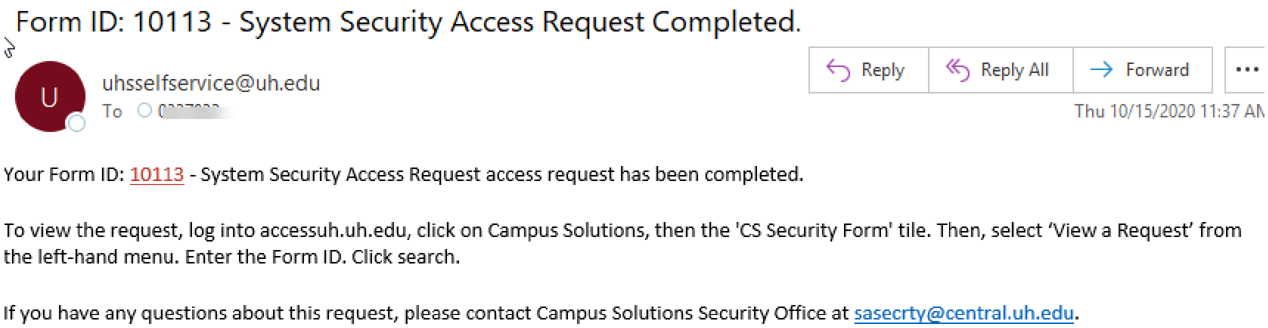
For more information, please see MAPP 10.08.02 Security Violations Reporting.

Action Items

2 rows

	Acknowledgement	
1	○ No	By switching 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.
2	○ No	Check here to confirm employee needs access to education records in order to perform their official educationally-related duties.

FYI. Upon clicking the submit button, the requester's Manager will receive a notification email like:



Form ID: 10113 - System Security Access Request Completed.

uhsselfservice@uh.edu

To 0[illegible]

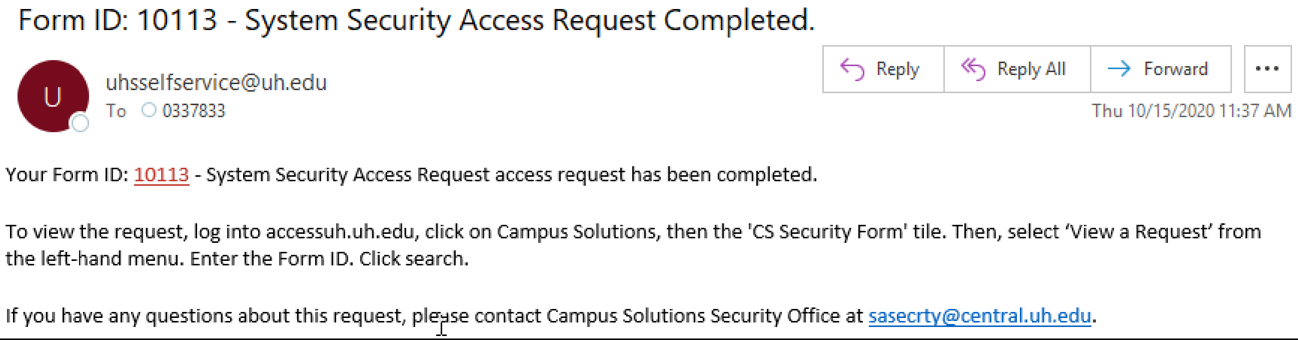
Thu 10/15/2020 11:37 AM

Your Form ID: 10113 - System Security Access Request access request has been completed.

To view the request, log into accessuh.uh.edu, 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 Campus Solutions Security Office at sasecrty@central.uh.edu.

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



Form ID: 10113 - System Security Access Request Completed.

uhsselfservice@uh.edu

To 0337833

Thu 10/15/2020 11:37 AM

Your Form ID: 10113 - System Security Access Request access request has been completed.

To view the request, log into accessuh.uh.edu, 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 Campus Solutions Security Office at sasecrty@central.uh.edu.