

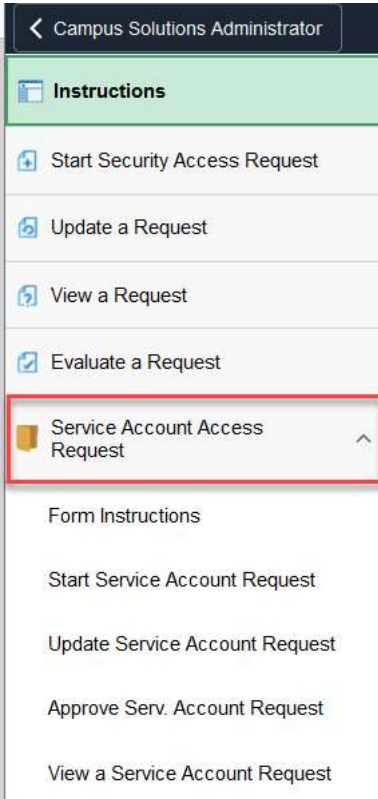
How to start a service account request for self?

1. Start by logging in to Campus Solutions

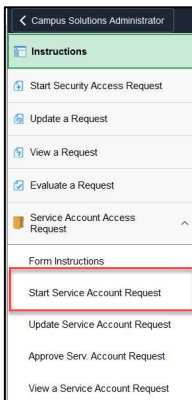


2. Look for your institution's security eForm icon. If you don't see the icon, please email your institution's CS security administrator with your PeopleSoft ID.

3. Click on the 'Service Account Access Request Folder'



4. Select 'Start Service Account Request'.



5. a. Validate the items 1-3 on this page.

- b. Enter the service account name in '4' and the CSS Lead for that business area in '5'.
- c. All current service accounts users of the requested account are listed in '6'

Before Campus Solutions Service Account access can be granted, the user must be an active employee or Person of Interest (POI).

For assistance with the form or security access questions, please email sa-security@uh.edu.

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	<input type="text"/>		
Name	<input type="text"/>	1	Campus ID
College/Department	<input type="text"/>		Job Title
Email Address	<input type="text"/>		Phone

Request Access For

2 Self Yes

Manager Name	<input type="text"/>	Manager PeopleSoft ID	<input type="text"/>
Manager Email	<input type="text"/>	Manager Phone	<input type="text"/>

3

Service Account Information

4 *SA Name


5 *UH CSS Lead

Current Service Account Users

Service Account Name ¹	Authorized User ID ¹	Authorized User Name ¹
1		6

6. Click 'Next'

7. Read and complete the Acknowledgement section by clicking the toggle from 'No' to 'Yes'. Click Submit. The form is then routed to the identified Manager for approval.

 Add a Request : Page 2

Request Access For

PeopleSoft ID Name

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 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 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 mis 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, 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 resources responsibly. Under State of Texas Department of Information Resources guidelines, systems not requiring unique user identification are exempt from this requirement.

Form Action Items

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.

Comments

8. You will receive an email like the one below when all approvers have approved your form.

UNIVERSITY of HOUSTON SYSTEM

Your Form ID: [172022](#) - Campus Solutions Access Request access request has been completed.

To view the request, log into AccessUH, click on Campus Solutions, then the Security Form folder, click the Service Account Request form. 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 sasectry@central.uh.edu