University of Houston

Campus Solutions System Security Access Request Form

Supervisory personnel must complete this form for the employee and Email the completed form to ALL appropriate Campus Security Administrators (CSA) for access/Role assignments, see pages 3-5.

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

1. Employee – a user, processed as an active employee thru Human Resources and has an employee ID number.
2. Non Employee or Person of Interest (POI) – a user who needs Campus Solutions access but is not an employee of the University. Sponsoring party has submitted this user as an active Person of Interest to Human Resources and has received a PeopleSoft ID number.
3. Mandatory training session required – for any access that requires pre-requisite training, the training must be indicated on the form with the date class was taken and the class session name.

Once they have the form, the CSA will obtain the module business owner's initial to confirm Roles to be assigned and scan form into the system for processing. The Supervisor and employee will receive an email when the form has been processed.

Check Yes for Short Term Access Request if access requested is for a limited time frame. Access will be terminated on end date.

{hort Term Access Request ☐ b2 ☐ ¸Ŝă

Start Date _____ End Date _____

Last Name: _____ First Name: _____ Middle: _____

Empl ID/PeopleSoft: _____ Job Title: _____

Empl UH Email: _____ Empl Campus Phone: _____ Coll/Dept. Name: _____

Display of SSN & Date of Birth

Set search screens to display ONE of the following:

☐ None ☐ Partial ☐ Full

Authorizing signature for "Full" Access:

Full display of SSN & DOB requires written justification from supervisor. Use this area. Full display is approved by the Office of Records and Registration.

Approvals (Both signatures below AND employee signature on Confidentiality Statement on page 2 are required)

Supervisor/Manager Signature: _____ Print Name: _____ Date: _____

Supervisor UH Email: _____ Supervisor Phone: _____

Coll/Dept Business Admin Signature: _____ Print Name: _____ Date: _____

Assistance Information

Training:			
Dolores Quiroz		832-842-8745	dequiroz@uh.edu
Help Desks:			
UH&UH System	IT Help Desk	713-743-1411	
UHCL	IT Help Desk	281-283-2484	uhclsac@uhcl.edu
UHV	IT Help Desk	361-570-4121	
Human Resources:			
Sandra Armstrong	Security Admin	713-743-1962	sgarmstrong@uh.edu
Finance			
Kirk Williams	Security Admin	713-743-8063	kawwilli4@uh.edu

UH Main Campus View Only Roles

(Module approved View Access granted to NEW users)

UHM_CS_AD_GENVIEW	-Student Admissions General Info
UHM_CS_BIODEMO_DATA_VIEW	-Campus Community Demographic Info
UHM_CS_BIODEMO_STDNT_VIEW	-Student Demographic Info
UHM_CS_CHECKLIST_VIEW	-Student Checklists
UHM_CS_COMMENT_VIEW	-Student Comments
UHM_CS_COMMUNICATION_VIEW	-Student Communications
UHM_CS_SF_STDNT_ACCT	-Student Financials Customer Accts
UHM_CS_SS_STU_CTR_VW	-Student Self Service Center
UHM_CS_SVCIND_VIEW	-Student Service Indicators

If user requires additional access, continue to page 3 and choose the Update Roles listed by module.

PLEASE NOTE: An automated process removes Campus Solutions access when a user transfers to a new Administrative Office, Academic Group, or Department or terminates from a position. Self-Service access to P.A.S.S. and Student Self-Service access will remain active and available.

PeopleSoft Campus Solutions Security Administrator Section

Date received: Primary Permission List Assigned: Sec Admin Signature: Date:

Print Name: Javaria Saeed, ERP App 2 Admin		713-743-8582	jsaeed@central.uh.edu
	James Glickman, Security Coord	713-743-8731	jglickma@central.uh.edu

Last Name: _____ First Name: _____ Middle Initial: _____

Empl ID/ PeopleSoft: _____

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 of ten 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.

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 right s 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 account s, 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 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 10.03.03 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: _____

Printed Name: _____

Campus Solutions System Security Access Request Form

Last Name: _____ First Name: _____ Middle Initial: _____

Empl ID/ PeopleSoft: _____

Module Selections (mark all modules where access by user is required, then mark functions within each module)

For use by CSA's only
+ Add Following Roles for
-- Remove only module ___

❒ AA Academic Advising ADV

Access needed	Training required & prerequisites
☐ Academic Advisement View & Work Academic Audits	**SAXUAA** Prerequisites: SAXVWI incl QRYRR

- Check-in Advisor - ☐ Advising Comments ☐ Check-in ☐ Admin
- Academic Audit - ☐ View & Run ☐ Update ☐ Overrides
- Checklist - ☐ View ☐ Update or ☐ Correct
- Comment - ☐ View ☐ Update or ☐ Correct
- Communication - ☐ View ☐ Update or ☐ Correct
- Service Indicator - ☐ View ☐ Update or ☐ Correct

☐ Other: _____

For information or assistance contact :
Sara Lee slee@uh.edu 713-743-1611
Academic Audit & Advising Appl Lead / CSA

Security Administrator/Business Owner Authorizing
Signature:_____ Date:_____
Print Name: Sara Lee, AA Application Lead EMPS team

❒ AD Admissions ADM

**Approval is required from the Assoc Dean of Graduate & Professional Studies

No security will be granted without first attending the required pre-requisite training sessions.

To sign up for training, cont act Dolores Quiroz at 832-842-8745 or email dequiroz@uh.edu

Once prerequisite training has been completed, submit the Student Security Access Request form to the Admissions Security Administrator for processing, then access will be granted.

Access needed (check ALL that apply)	**Training required & prerequisites**
☐ Entering Graduate Admission Applications	**SAAEGA** Enter Applications
☐ Maintaining Graduate Admission Applications	**SAAMGA** Maintain Applications
☐ Entering UnderGraduate Admission Applications (Includes Query Run Access)	**SAAEGA** Enter Decisions

Signatures required, if access selected

- Application Maintenance View ☐
- College Admissions Processors ☐
- Graduate Processors Prgm Cklist ☐
- Residency Processors ☐
- International Processors ☐
- International Student Worker ☐
- Senior Processors ☐
- Fee Processors ☐
- Graduate Decision Making Process** ☐

Prospects:

- Bauer Event Mgmt. ☐ . . . Anne Ness >> _____
- Cougar Friday. . . . ☐ . . Jeff Fuller >> _____
- Cougar Preview. . . ☐ . . Jeff Fuller >> _____
- THE EVENT . . . . . ☐ . . Jeff Fuller >> _____
- Destination Houston ☐ . . Jeff Fuller >> _____
- TAP EVENT . . . . . ☐ . Nancy Herron >>_____

Web Cards:

- Domestic Web Card . . . ☐ . . . . . Jeff Fuller >> _____
- International Web Card . ☐ . . . Jeff Fuller >> _____

- Student Groups ☐
- Student Worker ☐
- Service Staff ☐
- Recruiter/Counselor ☐
- Recruiter Setup ☐

- Service Indicator - ☐ View ☐ Update or ☐ Correct
- Checklist - ☐ View ☐ Update or ☐ Correct
- Comment - ☐ View ☐ Update or ☐ Correct
- Communication - ☐ View ☐ Update or ☐ Correct

☐ Other: _____

For information or assistance contact
Keisha Lyons kdlyons@uh.edu 713-743-1010
Admissions Module CSA

Security Administrator/Business Owner Authorizing
Signature:_____ Date:_____
Print Name: Djuana Young, Exec Director, Admissions

❒ CC Campus Community & Other UH System Access

- Operations Calendar - ☐ View ☐ Entry ☐ Admin
- External Organization - ☐ View
- Service Indicator - ☐ View ☐ Update or ☐ Correct
- Bio Demographic Data AddUpd ☐
- Bio Demo Student Data AddUpd ☐
- SF Bio Demographic Student - Address Only Update ☐
- IT Bio Demographic Student - Email Only Update ☐
- Health Data - ☐View ☐Update
- Police - View ☐
- HISD Ext Sys Data Upd/Correct ☐
- SEVIS - ☐ Setup ☐ Process

☐ Other: (incl. System Access) _____

Security Administrator/Business Owner Authorizing
Signature:_____ **Date:**_____
Print Name: Riod Triantoro, Analyst, Campus Community EMPS

For information or assistance contact :
Javaria Saeed jsaeed@central.uh.edu
James Glickman jglickma@central.uh.edu
Campus Solutions System Security

Last Name: _____ First Name: _____ Middle Initial: _____

Empl ID/ PeopleSoft: _____

***Module Selections** continued*

For use by CSA's only
+ Add Following Roles for
-- Remove only module ___

❒ **FA** **Financial Aid** SFA

**External departments must contact the Campus Security Administrator, Lew Herring, to determine which access/roles are to be assigned.

For information or assistance contact :
Lew Herring rlherring@uh.edu 832-842-4812
Financial Aid Module CSA

Security Administrator/Business Owner Authorizing
Signature:_____ Date:_____
Print Name:

❒ **SF** **Student Financials** SFS

- Query Read/Run ☐
- Checklist - ☐ View ☐ Update or ☐ Correct
- Comment - ☐ View ☐ Update or ☐ Correct
- Communication - ☐ View ☐ Update or ☐ Correct
- Service Indicator - ☐ View ☐ Update or ☐ Correct

☐ View
or
☐ Post
☐ Other: _____

The view status for SFS gives you the ability to view a student's account in SFS as an employee and as a student sees their account thru campus community. If you need group post of charges, you will need to go thru training. Please contact CSA.

For information or assistance contact :
Brandon Bob blbob@uh.edu 832-842-8895
Application Developer 2

Security Administrator/Business Owner Authorizing
Signature:_____ Date:_____
Print Name: Chris Durham, Application Developer III

❒ **SR** **Student Records** RAR (check ALL functions needed)

No security will be granted without first attending the required pre-requisite training sessions.
To sign up for training, cont act Dolores Quiroz at 832-842-8745 or via email at dequiroz@uh.edu.
Once prerequisite training has been completed, submit the Student Security Access Request form to the Student Records Security Administrator for processing, then access will be granted.

Access needed (check ALL that apply)	**Training required & prerequisites**
☐ View and Work with Student Records (includes Query Run access)	**SAXVWI** Prerequisites: none
☐ Place & Release Service Indicators (Stops)	**SAXSIB** (requires authorization from the Business Unit to which the Service Indicators belong) Prerequisites: SAXVWI
☐ Add and Drop Students from Classes	**SAREMB** Prerequisites: SAXVWI Recommended: SAXSIB (as you might be adding them to classes after removing certain stops)
☐ Modify Program Plan Stack (discontinued students, changing a student's plan, activating a student returning from suspension, adding student attributes, as well as solving common student issues associated with the program/plan stack)	**SAXSRW** Prerequisites: SAXVWI, SAREMB Recommended: SAXSIB (as you might be making these changes after removing certain stops)
☐ Update the Class Schedule (Curriculum Management)	**SARCMU** Prerequisites: SAXVWI, SAREMB

- Checklist - ☐ View ☐ Update or ☐ Correct
- Communication - ☐ View ☐ Update or ☐ Correct
- Comment - ☐ View ☐ Update or ☐ Correct
- Service Indicator - ☐ View ☐ Update or ☐ Correct

☐ Other: _____

For information or assistance contact :
Akash Bhatt abhatt@uh.edu 713-743-7370
Student Records Module CSA

Security Administrator/Business Owner Authorizing
Signature:_____ Date:_____
Print Name: Cassandra Heavrin Assoc.Registrar, SIS

Last Name: _____ First Name: _____ Middle Initial: _____

Empl ID/ PeopleSoft: _____

Module Selections Continued

For use by CSAs o nly
+ Add Following Roles for
-- Remove only module ___

❒ **IR** **Institutional Research, Coordinating Board Reporting, PeopleTools Query**

☐ CBM Other Processes/Reports _____

☐ IR Other Processes/Reports _____

--- For all other IR Access, please use the supplemental CB/IR Security Form ---

• Query Access - ☐ Create Only in Production **or** ☐ Create in Reporting

Other: _____

For information or assistance contact :
Susan Moreno semoreno@uh.edu 713-743-0640
Dir, Institutional Research/Coordinating Board Reporting
Marie Coleman macolem3@uh.edu 713-743-9762
Coordinating Board/IR Functional Analyst IV, EMPS Team

Security Administrator/Business Owner Authorizing
Signature:_____Date:_____
Print Name: Susan Moreno, Director, IR

❒ **ES** **Call Center**

• Call Center View - AD, FA, SF, SR ☐ • BioDemo Data Pier Update ☐

• Check-in System - ☐ Front Desk, ☐ Advisor, ☐ Admin ☐ Superuser

For information or assistance contact :
Veronica Avila vmavila@central.uh.edu 713-743-9651
Enrollment Services Call Center CSA

Security Administrator/Business Owner Authorizing
Signature:_____ Date:_____
Print Name: Pam Ogden, Manager Call Center