Student Administration Management

UHCL The choice is clear.

Campus Solutions System Security Access Request Form

SUPERVISORY PERSONNEL must complete this form. Consult with your supervisor and the Student Administration Management Team for Role assignments PRIOR to submitting the form for processing. **Note: This form is not for Financials or HR access.**

Before administrative security access can be granted in the E-Services/Campus Solutions (PeopleSoft) System, the user must have the following information to complete the form:

1. Employees – user has been processed as an active employee thru Human Resources and has received an employee ID number and a valid UHCL email address on file.

2. Non Employees or Person of Interest – Persons of Interest are users who need administrative access to the Campus Solutions System, but are not employees 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. Must read & sign the Confidentiality Statement.

4. Supervisor's signature authorizing requested access.

5. Submit completed form to samsecurity@uhcl.edu.

Employee Type

◯ Active Employee ◯ Active POI ◯ Student Worker/Work Study

New Hire?

◯ Yes ◯ No

New Hire Start Date

Short Term Access? Provide End Date.
All CS access will be removed on date provided.

Last Name

First Name

Department

Job Title

UHCL Email

Extension

User 7-Digit ID

Indicate Roles or Pages needed (Some access may require additional approval and/or training.)

or Copy access from User: **7-Digit ID** **User Name**

Data Access Display *Full SSN and Date of Birth access requires Registrar's approval.

SSN

◯ None ◯ Partial ◯ Full*

Date of Birth

◯ None ◯ Partial ◯ Full*

Business Owner Approval

FA Business Owner Signature

SF Business Owner Signature

Registrar Signature

Confidentiality Statement

I understand that data obtained from any UHS system is to be considered confidential and to NOT be shared with anyone not previously authorized to receive such data.

General Security Guidelines for Users Adapted from Computing Facilities User Guidelines (1/91)

The University Of Houston Department Of Information Technology exists to serve faculty, staff and students of the University in support of instructional and research activities. University computing facilities are a public resource and may not be used for personal or corporate profit. The following conditions apply to all users of the computing facilities.

(1) The user shall not seek or reveal information on, obtain copies of, or modify files, tapes or passwords belonging to other users, nor may the user misrepresent others. The user may only use his/her legal name or actual title at the University. Only one person may use a computer account, and that is the person to whom the account was granted.

(2) The user shall not make copies of copyrighted software.

(3) The user shall not use the resources provided by the University for purely recreational or trivial purposes.

(4) The user shall not develop or use programs that harass other users or damage and/or alter the operating system or other existing software.

(5) The user shall not engage in deliberately wasteful practices such as printing large amounts of unnecessary output, performing unnecessary computations, simultaneously queuing multiple batch jobs and holding unused tape drives and telephone lines.

(6) The user shall not engage in behavior that creates an unpleasant environment for other users.

Violations of these conditions are unethical and may be violations of University policy and/or criminal offenses. Users are expected to report any suspected violations to the Customer Services Help Desk at 713-743-1411. When possible violations are reported or discovered, Information Technology reserves the right to investigate the possible abuse. Certain members of Information Technology may be given the authority to examine files, passwords, accounting information, printouts, tapes or other materials that may aid in the investigation. While an investigation is in progress, access to computing resources may be suspended for the individual or account in question. When possible unauthorized use of computing resources is encountered, Customer Services shall notify the user. Should unauthorized use continue after notification of the user, the matter shall be brought to the attention of the Vice President of Information Technology, which could result in cancellation of access privileges, disciplinary review, expulsion from the University, termination of employment and/or legal action. (For a complete copy of these guidelines, see the University of Houston Computing Facilities User Guidelines (1/91) and the Texas Computer Crimes Statute--Section 1, Title 7, Chapter 33, Texas Penal Code.)

State law requires that you be informed of the following:

(1) with few exceptions, you are entitled on request to be informed about the information the university collects about you by use of this form;

(2) under sections 552.021 and 552.023 of the Government Code, you are entitled to receive and review the information; and

(3) under section 559.004 of the Government Code, you are entitled to have the University correct information about you that is incorrect.

Student Administration Application Privacy Warning

I understand that most student information is classified as confidential under the Family Education Rights and Privacy Act of 1974. Student's records are released for use by faculty and staff for authorized campus-related purposes on a need-to-know basis. The release of records for non-campus, non-academic or no administrative use occurs only with the student's knowledge and consent or where required by law or when subpoenaed.

I understand that public information on a record that may be released upon request includes name, address, telephone number, date of birth, major and minor fields of study, dates of attendance, degree(s) received, the most recent previous educational institution attended, and participation in officially recognized activities and sports, weight and height for athletes only. (Students who do not wish this information to be released are responsible for notifying UHS.) Presence of a "Withhold Public Information" flag within a system indicates that no information regarding the student can be released without the student's permission.

I have read and understood the information on this form. I agree to comply with the rules as stated therein:

Employee's Signature	**Print Name**	**Date**

By signing this form I am authorizing the requested access.

Supervisor Signature	**Supervisor Print Name**	**Date**

Supervisor Title	**Supervisor UHCL Email**	**Supervisor Extension**

For SAM use only: Campus Security Administrator Signature

Date Received

Access Added: *Additional Assigned Roles and Data Permissions attached.*