University of Houston Systems

CoogPlan Access Request

Complete the top part of this form; read and sign the security agreement on the back, and return the form to your supervisor. Before you can access the CoogPlan/Hyperion Budget Planning System.

1. You must have a CougarNet account.
2. You must have completed CoogPlan training.
3. Give this form to your department business administrator or your manager. The form should be scanned and sent to srmohiuddin@central.uh.edu or the Budget Office.

Completed By Applicant:

Access Action: Add Change Delete

Cougarnet ID: EMPLID: Job Title:

Last Name: First Name: Middle Initial:

Campus: College Id/Name: Dept Id/Name:

List desired DEPT ID below in boxes provided and check desired security role or action.

DEPT ID (Hxxx, Sxxx)	Budget View Only	End User	End User Special Access	Remove Access
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐

Departmental Approvals:

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

College/Division Business Administrator Signature:_____ Print Name:_____ Date:_____

Employee Signature:_____ Print Name:_____ Date:_____

Budget Office: For Office Use Only

Date Training Completed if applicable: _____

Budget Office Signature: _____ Name: _____ Date: _____

Security User Groups: _____

CoogPlan Administrator (713.743.4397): For Office Use Only

CoogPlan Signature: _____ Name: _____ Date: _____

Security User Groups: _____

Comments:

_____

_____

_____

_____

Confidentiality Statement

University of Houston Systems

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.)

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 _____